

جريمة التزوير الإلكتروني في التشريع الأردني

(دراسة مقارنة)

The crime of electronic forgery in the Jordanian legislation

Comparative Study

إعداد

عمر عبد السلام حسين الجبوري

إشراف

الدكتور أحمد اللوزي

قدمت هذه الرسالة إستكمالاً لمتطلبات الحصول على درجة الماجستير في

القانون العام

قسم القانون العام

كلية الحقوق

جامعة الشرق الأوسط

أيار –2017

ب

تفويض

أنا الطالب عمر عبد السلام حسين أفوض جامعة الشرق الأوسط بتزويد نسخ من رسالتي ورقياً وإلكترونياً للمكتبات ، أو الهيئات و المؤسسات المعنية بالأبحاث و الدراسات العلمية عند طلبها.

الأسم : عمر عبد السلام حسين

التاريخ : ٢٢ / ٥ /2017 م

التوقيع :

قرار لجنة المناقشة

نوقشت هذه الرسالة وعنوانها " جريمة التزوير الإلكتروني في التشريع الأردني (دراسة مقارنة)".

وأجيزت بتاريخ ١٦ / ٥ / ٢٠١٧م

أعضاء لجنة المناقشة		التوقيع
١- الأستاذ الدكتور نزار العنبكي	رئيساً وعضواً داخلياً	
٢- الدكتور صالح حجازي	عضو خارجي	
٣- الدكتور أحمد اللوزي	مشرفاً	



شكر والتقدير

انطلاقا من قول نبينا الكريم محمد عليه وعلى اله وصحبه الطيبين الطاهرين أفضل الصلاة والسلام :(من لا يَشكُر الناس لا يَشكُر الله).

بعد التوجه بالشكر و الثناء لصاحب النعمة العلي الأعلى ، لما تفضل به علي من وافر نعمته وعطائه ، اتقدم بجزيل الشكر والامتنان لأستاذي الفاضل الدكتور أحمد اللوزي لتفضله مشكوراً لأشراف على هذه الرسالة.

كما ويشرفني أن أتقدم بالشكر الجزيل وبلسان يعجز عن التعبير لأساتذتي في كلية القانون في جامعة الشرق الأوسط و أخص منهم أعضاء لجنة المناقشة على تشريفي بقبولهم قراءة هذه الرسالة ومناقشتي في مندرجاتها ، أن يجدو في ثناياها ما يؤلف إضافة جديدة إلى المكتبة القانونية العرا قية والأردنية، وان يجدو لي عذرا فيما تنطوي عليه من مآخذ أفرزتها حداثة تجربتي في البحث القانوني ولا يفوتني أن أتقدم بالشكر لمن حرمتني آفة النسيان عن ذكر اسمه.

الباحث

الإهداء

إلى من كلله الله بالهيبة والوقار ...

إلى من أحمل اسمك بكل أفتخار...

إلى من غرس جذور العزم و الإصرار...

إلى من علمني العطاء بدون انتظار ...

والدي .....

إلى ملاكي في الحياة ...

إلى معنى الحب وإلى معنى الحنان والتفاني ...

إلى بسمة الحياة وسر الوجود...

إلى من كان دعائها سر نجاحي وحنانها بلسم جراحي ...

أمي ......

إلى من أظهروا لي ما هو أجمل من الحياة ...

إلى من كانوا ملاذي وملجئي...

إلى من تذوقت معهم أجمل اللحظات...

إلى من سأفتقدهم ...

أخوتي

أهدي لكم عملي المتواضع هذا

مع المحبة والعرفان

الباحث

فهرس المحتويات

جريمة التزوير الإلكتروني في التشريع الأردني (دراسة مقارنة)

إعداد

عمر عبد السلام حسين الجبوري

إشراف

الدكتور أحمد اللوزي

الملخص

وقفنا في هذه الدراسة على بيان ماهية جريمة التزوير الإلكتروني ومفهوم جريمة التزوير الإلكتروني وتعريفه ، وكذلك بيان طبيعة جريمة التزوير وتطورها في ضوء ظهور الشبكة المعلوماتية ، كما تسعى هذه الدراسة إلى بيان الصيغ التشريعية في القانون الإردني و التشريعات المقارنة لجريمة التزوير الإلكتروني من أجل بيان إمكانية إنطباق نصوص قانون العقوبات على الجرائم الإلكترونية أم تحتاج إلى قوانين خاصة بها.

واستخدم الباحث في هذه الدراسة المنهج الوصفي التحليلي المقارن من خلال وصف ومقارنة ما جاء في القوانين الجزائية الأردنية وكذلك ما جائت في القوانين الجزائية المقارنة المتعلقة بموضوع جريمة التزوير الإلكتروني وتعديلاتهم السارية المفعول.

وإن الإحاطة بهذا الموضوع استلزم البحث في الإطار العام للدراسة من حيث الإشكالية العامة وأهميتها و اهدافها ومحددات الدراسة ، كما بينا النموذج القانون لجريمة التزوير الإلكتروني وكذلك صور الخاصة لجريمة التزوير الإلكتروني في التشريع الأردني والتشريعات المقارنة ، وكذلك بيان الإجراءات القانونية الخاصة لجريمة التزوير الإلكتروني سواء كانت هذه الإجراءات تنظيمية

كأمور المتعلقة بتحديد الأختصاص أو المحاكم المختصة بالنظر في مثل تلك الجرائم ، وكذلك بيان العقوبات المقررة لجريمة التزوير الإلكتروني في القانون الأردني والقوانين المقارنة.

ومن خلال هذه الدراسة توصل الباحث إلى أهم التوصيات التي يوصي بها ، وهي إعتماد مبدأ النظير الوظيفي في الصيغ التشريعية لإمكانية التعامل بالمحرر الإلكتروني مقارنة بالمحرر الورقي ، وساواتها بها من حيث القيمة القانونية في الإثبات من خلال الإسترشاد بما نص عليه قانون الأونسترال في هذا المجال ، العمل على الاقتداء بالدول المتقدمة و التعاون معها في مجال التكنولوجيا و الاستفادة من خبراتها في تشريع القوانين التي تعالج الجرائم الإلكترونية وخصوصا جرائم التزوير الإلكتروني ، وكذلك العمل على إنشاء جهاز أمني مختص في معالجة ومكافحة مثل تلك الجرائم الإلكترونية.

الكلمات المفتاحية: التزوير الإلكتروني ، الجرائم الإلكترونية ،المحرر الإلكتروني.

The crime of electronic forgery in the Jordanian legislation Comparative Study

Prepared by

Omar Abdulsalam Hussein

Supervised by

Dr.Ahmed al Lozi

Abstract

In this study, we discussed the nature of the crime of electronic forgery and the concept of the crime of electronic forgery and its definition, as well as the nature of the crime of forgery and its development in the light of the emergence of the information network. This study also seeks to explain the legislative formulas in Jordanian law, The provisions of the Penal Code on cybercrime or need their own laws.

In this study, the researcher used the comparative descriptive analytical method by describing and comparing the Jordanian penal laws as well as the comparative penal laws related to the subject of electronic forgery and their amendments.

The study also examined the legal framework for the crime of electronic forgery as well as the special images of the crime of electronic forgery in the Jordanian legislation and the comparative legislations, as well as the statement of the special legal procedures for the crime of electronic forgery, whether these The procedures are organized as matters relating to the determination of jurisdiction or courts competent to deal with such crimes, as well as the statement of the penalties prescribed for the crime of electronic forgery in the law and comparative laws.

Through this study, the researcher reached the most important recommendations that he recommends, namely, the adoption of the

principle of functional counterpart in the legislative formulations of the possibility of dealing with the electronic editor compared to the paper editor, and its legal validity in terms of the legal value of the evidence through the guidance of the UNCITRAL law in this field, To follow the example of developed countries and cooperate with them in the field of technology and to benefit from their expertise in the legislation of laws that deal with electronic crimes, especially electronic forgery, as well as work on the establishment of a specialized security in the treatment and control of such cyber crimes.

Key words :electronic forgery, cybercrime, E-editor.

الفصل الأول

الإطار العام للدراسة

المقدمة :

تعتبر جرائم التزوير من أدق الموضوعات في نظام العقوبات المعاصرة ، فجرائم التزوير من أخطر الجرائم التي تخل بالثقة الواجب توافرها بين أفراد المجتمع فهناك ترابط بين جرائم التزوير وما يترتب عليها من آثار دينية و اجمتاعية و اقتصادية ، فهي تساعد على انتشار الفساد بكل أنواعه ، ولهذا فأن الأديان السماوية منذ استخلف الله الإنسان على وجه الأرض تؤثم التزوير وتنكره ، حتى إن الشريعة الإسلامية تناولت هذه الجرائم باعتبارها منكرا يتعين سن قانون يعاقب عليه حماية للفرد و المجتمع.

احتلت جريمة التزوير بشكل عام أهميه بالغة في التشريعات القانونية على مختلف العصور، ولا سيما التشريعات الجزائية الحديثة التي حددت أركان وصور جريمة التزوير والعقوبات الواجب إنزالها عليها. وتماشيًا مع ما تقدم قام المشرع الأردني بتنظيم أحكام جريمة تزوير المحررات في المواد (260-272) من قانون العقوبات الأردني رقم (16) لسنة 1960 تحت عنوان الجرائم المخلة بالثقة العامة[(1)].وكذلك المشرع العراقي قام بتنظيم أحكام جريمة التزوير في المواد (286 - 301) من قانون العقوبات العراقي رقم (111) لسنة 1969 في الفصل الثالث تزوير المحررات[(2)]، وتتكون جريمة التزوير بصورة عامة من ركن المادي و ركن المعنوي ، فهما اساس النظرية العامة لهذه الجرائم بحيث يتوجب توفرهما معاً قبل البحث في بيان تحقق أي جريمة

---

(1)قانون العقوبات الأردني ، رقم 16 ، لسنة 1960 ، المادة (16).

(2)قانون العقوبات العراقي ، رقم 111 ، لسنة ، 1969 المادة (286).

من جرائم التزوير المتنوعة ، ويقصد بالركن المادي لجريمة التزوير بأنه تحريف أو تغيير للحقيقة وأن يتم ذلك بإحدى الطرق المنصوص عليها في القانون حصرا ولا يشترط أن يكون التغيير كليا، أي ابدال كل البيانات بما يخالف الحقيقة، ويكفي أن يكون تغيير الحقيقة جزئيا او نسبيا، ويقع في الغالب على المحررات، أما الركن المعنوي فيتخذ صورة القصد الجنائي والذي يتمثل وبصورة مختصرة بالعلم والإرادة في ارتكاب جريمة التزوير ، وكذلك لابد ان يتوفر عنصر الضرر الذي يعتبر ايضاّ من الاركان الاساسية لجريمة التزوير ، وذلك أن جريمة التزوير لا عقاب عليها إن لم يكن هناك ضرر يلحق بالغير [1].

أما التزوير في محررات عبارة عن تغيير الحقيقة مهما كانت وسيلته وأياً كان موضوعه، يلجأ اليه الجاني بهدف غش المجني عليه والاحتيال عليه، وهذه الفئة من الجرائم دائما تهدف الى وحدة المصلحة المعتدى عليها وبصورة مباشرة وهي الثقة العامة التي يضعها أفراد المجتمع في بعض الاشياء أو القيم أو المحررات ذات الأهمية القانونية والتي تعتبر في نفس الوقت أدوات لا يمكن الاستغناء عنها في تسيير الحياة اليومية للأفراد [2] .

وهناك ايضاّ ما يسمى بالمحرر الإلكتروني الذي يكون عبارة عن مجموعة من العلامات والرموز تعبر اصطلاحا عن مجموعة مترابطة من الأفكار والمعاني الصادرة عن شخص او اشخاص معينين ، وهو في جوهره كتابة مركبة من حروف وعلامات تعبر عن معنى أو فكرة معينة[3].

---

(1)حسني، محمود نجيب ،(1988)، شرح قانون العقوبات ، القسم الخاص ، دار النهضة ، القاهرة ص 14 .

(2) القهوجي, علي عبد القادر, (2002), جرائم الاعتداء على المصلحة العامة وعلى الانسان والمال – القسم الخاص – منشورات الحلبي الحقوقية، بيروت, ص 93.

(3)عرب ، يونس , (2002) ، دليل أمن المعلومات والخصوصية – جرائم الكمبيوتر والانترنيت، الطبعة الاولى، اتحاد المصارف العربية ، الجزء الاول، عمان، ص437.

وإن ازدياد نسبة التعامل بهذه الوثائق كان له دور ايجابياً في تقليص التكاليف و الوقت والحد من التضخم الورقي ، وتحسين آداء الخدمة للمتعامل ، لكنه في نفس الوقت حمل معه مخاطر الاعتداءات على هذا النوع من المحررات في أشكالها المستحدثة استفادت من تكهنولوجيا المعلومات و الإتصالات في اتجاه سلبي و غير مشروع.

وتنبهت العديد من التشريعات الجزائية المقارنة الى سلوكيات المستحدثة في جرائم التزوير التي عكستها تقنية نظم المعلومات، واستطاعت أن تتخطى المفهوم التقليدي للتزوير وعاء ومحل التزوير، وحسناً فعل بالنظر الى ضخامة الجرائم الإلكترونية و أهميتها، واتساع نطاق استعمالها.

مشكلة الدراسة :

تتمثل نقطة البدء في بحث هذا الموضوع في أن جريمة التزوير الإلكتروني و التي تعتبر من الجرائم المستحدثة والتي تثار فيها الكثير من المشاكل سواء كان على المستوى المحلي أو الدولي، سواء من ناحية كفاية النصوص التقليدية في محاربة مثل تلك الجرائم الإلكترونية أو القيام بتشريعات جديدة تواكب تتطور مثل تلك الجرائم. ويتفرع عن هذه الإشكالية التساؤلات التالية :

1- ما المقصود بالتزوير الإلكتروني وما حكمه وأركانه والاثار الناتجة عنه في التشريع الأردني والتشريعات المقارنة ؟

2- هل من الإمكان انطباق نصوص جريمة التزوير التقليدية على التزوير الإلكتروني ؟

3- هل تجريم تزوير الإلكتروني بصفة عامة يحتاج إلى نص جزائي خاص؟

4- هل تعتبر الآليات و الإجراءات المتبعة في مكافحة جريمة التزوير الإلكترونية كافية لردع هذه الجريمة؟

أهداف الدراسة :

تأتي هذه الدراسة لتحقيق الأهداف التالية:

1- بيان ماهية التزوير الالكتروني وأركانه والآثار الناتجة عنه.

2- بيان إمكانية انطباق النصوص الجزائية لجريمة التزوير التقليدية على جريمة التزوير الإلكتروني أم تحتاج الى قانون خاص.

3- بيان هل من إمكانية وضع قانون خاص لجريمة التزوير الإلكتروني.

4- بيان الآليات والاجراءات المتبعة لمكافحة جريمة التزوير الإلكتروني.

أهمية الدراسة :

تكمن أهمية هذه الدراسة في تناولها لظاهرة مستحدثة وهى ظاهرة جرائم الإلكترونية وخاصة جريمة التزوير الإلكتروني منها، فالتطور التكنولوجي على الرغم من آثاره الإيجابية إلا أن له العديد من السلبيات التي تهدد أمن واستقرار المجتمع وخاصة جريمة التزوير الإلكتروني التي تعمل على الإخلال بالثقة العامة ليس في الأردن فقط بل في العالم بأسره.

ومع ازدياد وتطور هذا الجرائم وخاصة جريمة التزوير الإلكتروني في المجتمعات الدولية تكمن أهميتها فيما يلي :

1- البحث في الأنظمة القانونية الإلكترونية المطبقة في المملكة الأردنية الهاشمية والمقارن مع التشريعات الأخرى ، لمواجهة مثل تلك الجرائم الخطيرة التي تؤدي الى الإخلال في الثقة العامة.

2- التصدي لمثل تلك الجرائم وذلك لاتصافها بالاستمرار والتجديد في أنشطتها.

3- كما تنبع أهميتها من حاجة التشريعات،الى القاء الضوء على مثل هذا النوع من الجرائم الذي يحمل الكثير من الآثار السلبية، التي تهدد أمن وسلامة المجتمع.

حدود الدراسة :

إن هذه الدراسة تحدد بالأبعاد التالية :

1- الحدود المكانية: إن الجرائم الإلكترونية وخاصة جريمة التزوير الإلكتروني حيث توجد فيها صعوبة في تحديد الحيز المكاني، لأن مثل تلك الجرائم لا توجد حدود محددة فيها فهي تمتد لتشمل مناطق جغرافية خارج حدود الدولة لذلك يصل مداها الى دول اخرى، كما يختلف ايظاً القوانين والعقوبات بين قوانين تلك الدول. وهذه الدراسة سوف تتطرق الى تشريعات المملكة الأردنية الهاشمية و التشريعات المقارنة.

2- الحدود الزمانية: فهي تبدأ منذ أن وضِعَ قانون العقوبات الأردني رقم 16 لسنة 1960، وقانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015، وقانون العقوبات العراقي رقم 111 لسنة 1969 .

3- الحدود الموضوعية: تتحدد الدراسة في بيان مفهوم جريمة التزوير الإلكتروني وأركانها و الطرق التي تؤدي الى ارتكابها،والجهة المختصة بالنظر والفصل فيهما، وبيان العقوبات المقررة لها في التشريعات المقارنة.

مصطلحات الدراسة :

1- التزوير: عرفت المادة (260) من قانون العقوبات الأردني لسنة (1960) بأنه " هو تحريف مفتعل للحقيقة في الوقائع والبيانات التي يراد إثباتها بصك أو مخطوط" [1] .

2- تغيير الحقيقة: هو السلوك الإجرامي الذي يقوم به التزوير فاذا انتفى انتفت الجريمة. ولا يشترط أن يكون التغيير كليا، أي إبدال كل البيانات بما يخالف الحقيقة، ويكفي أن يكون تغيير الحقيقة جزئيا أو نسبيا، والمستقر في الفقه أن المقصود في التزوير، ليس تغيير الحقيقة الواقعية المطلقة، إنما تغيير الحقيقة النسبية التي تلحق ضرر الطرف الأخر[2]

3- التزوير الإلكتروني: فهو أي تغيير للحقيقة يرد على مخرجات الحاسب الألي سواء تمثلت في مخرجات ورقية مكتوبة كذلك التي تتم عن طريق الطابعة وكانت مرسومة عن طريق الرسم ويستوي في المحرر المعلوماتي ان يكون مدوناً باللغة العربية محفوظة على دعامة لبرنامج منسوخ على اسطوانة وشرط ان يكون المحرر المعلوماتي ذا أثر أثبات حق واثر قانوني معين[3].

4- المحرر الإلكتروني: المحررات في بيئة الحاسب الآلي بيانات ومعلومات ذات معنى لا تدركها الحواس وإن أمكن معرفتها إدراك محتواها وتداولها باستخدام أجهزة العرض والإخراج التقنية الخاصة، وهي ذات صيغة معنوية ولهذا اختلف الفقه حول وقوع جريمة التزوير عليها[4].

---

(1)قانون العقوبات العراقي رقم 111 لسنة 1969.

(2)يونس عرب ، دليل أمن المعلومات والخصوصية – جرائم الكمبيوتر والانترنيت ، ص2.

(3)حجازي ، عبد الفتاح بيومي ، (2002) ، الدليل الجنائي والتزوير في جرائم الكومبيوتر والانترنت ، دار الكتب القانونية، القاهرة، ص 170.

(4)المناعسة ، أسامة أحمد ، والزعبي جلال محمد ، (2014) ، جرائم تقنية نظم المعلومات الإلكترونية (دراسة مقارنة) – دار الثقافة ، عمان ، ص 66 .

الاطار النظري :

- الفصل الأول : وهو عبارة عن الاطار العام للدراسة ، يستعرض فيه الباحث مقدمة عن موضوع الدراسة وعرض لمشكلة الدراسة واهدافها واهميتها ، وكذلك حدود الدراسة المكانية والزمانية و الموضوعية ، ووأهم المصطلحات الواردة في الدراسة ، وايضاً يستعرض الباحث بعض من الدراسات السابقة ومايميز الدراسة الحالية عنها ، ومنهج الدراسة المتبع والاطار النظري لتقسيم الدراسة.

- الفصل الثاني : سيتناول الباحث في هذا الفصل ماهية التزوير الإلكتروني الذي يبين مفهوم التزوير الإلكتروني وتعريفه لغة وفقهاً وقانوناً ، وكذلك بيان خصائصه وطبيعته، و أيضاً بيان الصيغ التشريعية لجريمة التزوير الإلكتروني فيما إذا يحتاج إلى قانون خاص به أو إمكانية إنطباق القوانين التقليدية عليه ، لاسيما و أن التزوير الإلكتروني يختلف عن التزوير التقليدي من حيث طرق التزوير وكذلك من حيث محل التزوير ، ، إضافة إلى ذلك سيتطرق الباحث الى بيان النموذج القانوني لجريمة التزوير الإلكتروني الذي يتكون من ركن المادي لجريمة التزوير الإلكتروني الذي يقصد به وقوع نشاط إجرامي من شأنه تغيير الحقيقة في محرر بطرق التي ينص عليها القانون ، أما الركن المعنوي لجريمة التزوير الإلكتروني الذي يتخذ صورة القصد الجزائي الذ ينحصر في أمرين وهو علم الجاني والأردة المتولدة فيه لرتكاب الجريمة وركن الخاص لجريمة التزوير الإلكترونية الذي يتمثل بضرر الذي يحصل بسبب وقوع الجريمة .

- الفصل الثالث : سيبين الباحث في هذا الفصل صور جريمة التزوير الإلكتروني وحصر الباحث في هذا الفصل صورتان من صور جريمة التزوير الإلكتروني ، حيث تطرق

الباحث في الصورة الأولى لجريمة التزوير الإلكتروني هي جريمة تزوير التوقيع الإلكتروني وبيان مفهوم التوقيع الإلكتروني وتعريفه في التشريعات المقارنة وبيان صوره وكذلك حجية التوقيع الإلكتروني في التشريعات المقارنة ، إضافة إلى ذلك بيان الحماية الجزائية للتوقيع الإلكتروني من التزوير و بيان خصائص جريمة تزوير التوقيع الإلكتروني ، أما صورة الثانية لجريمة التزوير الإلكتروني هي جريمة تزوير بطاقة الائتمان حيث تطرق الباحث إلى بيان مفهوم البطاقة الائتمانية وتعريفها في التشريعات المقارنة وبيان أنواع البطاقة الائتمانية ، إضافة إلى ذلك بين الباحث الحماية الجزائية لبطاقة الائتمان سواء على المستوى الدولي أو على مستوى التشريعات المقارنة.

- الفصل الرابع : سيتناول الباحث في هذا الفصل الإجراءات القانونية الخاصة لجريمة التزوير الإلكتروني ، حيث تطرق الباحث في هذا الفصل عن الإجراءات التنظيمية للحماية الخاصة لجريمة التزوير الإلكتروني حول الأليات المفروض أتباعها في سبيل صياغة احكام قانونية التي تعمل على ردع مثل تلك الجرائم والتي من خلالها تًعطى للمحاكم الحق في النظر في القضايا الناشئة عن عمليات التزوير الإلكتروني وهذا ما جرى بحثه في أمرين مهمين وهما ، الأمر الأول تم بيان المبادئ المتعلقة بتحديد الاختصاص بالنظر في جرائم التزوير الإلكتروني أما الأمر الثاني المحاكم المختصة بالنظر في جرائم التزوير الإلكتروني ، و أيضاً تطرق الباحث إلى الاجراءات التطبيقية للحماية الخاصة لجريمة التزوير الإلكتروني وذلك من خلال بيان دور الضابطة العدلية في مواجهة جرائم الكمبيوتر ، وكذلك بيان دور القاضي في تقييم الادلة الخاصة بجرائم

الكمبيوتر ، إضافة إلى ذلك تطرق الباحث إلى العقوبات المقررة لجريمة التزوير الإلكتروني في التشريع الأردني وكذلك في التشريعات المقارنة.

- الفصل الخامس : يخصص هذا الفصل لنتائج الدراسة وتقديم المقترحات وأهم التوصيات، وكذلك يحتوي على المراجع الخاصة بهذا البحث.

الدراسات السابقة :

من اهم الدراسات ذات الصلة بموضع الدراسة ما يلي :

1. دراسة حجازي, عبد الفتاح بيومي (2002)[1] , بعنوان: "الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت: دراسة متعمقة في جرائم الحاسب الآلي والإنترنت, دار الكتب القانونية, القاهرة. هدفت الدراسة إلى التعريف على كيفية الدليل الإلكتروني في جرائم التزوير باستخدام الكمبيوتر والإنترنت, وهي دراسة وصفية مكتبية, وقد استخدم الباحث المنهج الوصفي, وقد توصلت الدراسة إلى نتائج من اهمها: وجود صعوبات تواجه عملية استخلاص الدليل الإلكتروني في الجريمة المعلوماتية من أهمها: نقص خبرة أجهزة العدالة بصفة عامة, ونقصها لدى الأجهزة الأمنية بصفة خاصة, فيما يتعلق بثقافة الحاسب الآلي وتقنياته في مختلف مناحي الحياة قياساً بالدول الغربية, حيث إن امتلاك رجال الأمن للمهارات الشرطية في التحقيق التي طالما أسعفتهم في التصدي للجرائم التقليدية لن تكون ذات فائدة تذكر عندما يتعلق الأمر بالتحقيق في جرائم الحاسب الآلي والإنترنت؛ لأن الأخيرة تتصف بطابع تقني خاص يميز أدلتها, وطرق الكشف عن مرتكبيها, تمييزاً كبيراً عن مثيلاتها في الجرائم التقليدية.

---

(1)حجازي, عبد الفتاح بيومي, (2002), الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت: دراسة متعمقة في جرائم الحاسب الآلي والإنترنت, دار الكتب القانونية, القاهرة.

وتختلف هذه الدراسة عن دراستنا الحالية بانها تناولت بعض جوانب التزوير في جرائم الكمبيوتر والإنترنت، وركزت على الدليل الجزائي أيضاً بينما تناولت دراستنا الحالية مقارنة موقف المشرع الأردني والعراقي من جريمة التزوير الإلكتروني.

2. دراسة السراني, عبدالله بن سعود محمد, (2011)[1], بعنوان: فعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني, جامعة نايف العربية للعلوم الأمنية, الرياض. اشتملت الدراسة على خمسة فصول بالإضافة إلى المراجع والملاحق, وقد انطلقت فكرة هذه **الدراسة من** سعيها لإثبات فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني في ضوء انتشار التعاملات الإلكترونية التي تكتنفها خطورة لجوء بعض الملمين باستخدام التقنية في القيام بعمليات تزوير إلكترونية من شأنها أن تقلل من مصداقية التعاملات الإلكترونية في ضوء انخفاض قدرة الأساليب التقليدية على مواجهة هذه الجرائم, وعدم قناعة الجهات القضائية بالأدلة الرقمية والإلكترونية كوسائل إثبات يقينية وتذرعها بإمكانية تزوير الأدلة الإلكترونية, وعدم قناعتها التامة بيقينية هذه الأدلة في ضوء تذرع بعض المخول لهم باستخدام النظام ممن يرتكبون جرائم التزوير باستخدام آخرين للجهاز نتيجة تركه يعمل أثناء قضاء بعض مهام العمل الأخرى.

وتختلف هذه الدراسة بتناولها لمواضيع اثبات جريمة التزوير الالكتروني، بينما تناولت دراستنا مقارنة موقف المشرع الأردني والعراقي من جريمة التزوير الإلكتروني .

---

(1)السراني, عبدالله بن سعود محمد, (2011), فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني, جامعة نايف العربية للعلوم الأمنية, الرياض, ط1.

3. دراسة براهمي, حنان (2014)[1]، بعنوان: جريمة تزوير الوثقية الرسمية الإدارية ذات الطبيعة المعلوماتية, أطروحته دكتوراه غير منشورة، جامعة محمد خضير بسكرة، كلية الحقوق والعلوم السياسية قسم الحقوق، الجزائر. هدفت هذه الدراسة الى بيان تأثير المعلوماتية على الأنظمة القانونية من حيث أسباب الظهور المعاملات الإلكترونية، وهدفت ايضاً تحديد مفهوم الوثيقة المعلوماتية، وبيان القيمة القانونية والصيغة التشريعية لها في تجريم الوثيقة المعلوماتية، وكذلك تحديد أركان جريمة التزوير بالوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية، والعقوبات المقررة لها. وقد استخدم الباحث المناهج التالية الاستدلالي, و الجدلي، والمقارن.

واختلفت الدراسة الحالية عن الدراسة السابقة في بيان مفهوم الوثيقة المعلوماتية تشريعيا وفقهيا، واعتبار الوثيقة دليل إثبات وذات قيمة ثبوتية باعتبار أن جريمة التزوير لا تقع إلا إذا كان لهذه الوثيقة قيمة قانونية. وهذه الدراسة تبين جريمة التزوير الالكتروني في التشريع الاردني والعراقي.

4. دراسة القاضي, محمد عايد قفطان (2014)[2] بعنوان: القصد الجرمي في تزوير التوقيع الإلكتروني, رسالة ماجستير غير منشورة, جامعة جدارا, الأردن. تناولت هذه الدراسة موضوع القصد الجرمي في جريمة مستحدثة, ألا وهي جريمة تزوير التوقيع الإلكتروني, أما الفصل الأول فقد تم تقسيمه إلى مبحثين رئيسيين, خصص المبحث الأول لبيان ماهية التوقيع الإلكتروني, أما المبحث الثاني فقد تضمن ماهية الجريمة الواقعة على التوقيع الإلكتروني, وهي جريمة التزوير واختلافها عن جريمة تزوير التوقيع التقليدي, أما الفصل الثاني فقد تناول في المبحث الأول منه الركن المادي لجريمة تزوير التوقيع الإلكتروني, أما المبحث الثاني فقد

---

(1)براهمي ، حنان ، (2014) ، جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية ، أطروحة لنيل شهادة الدكتوراه ، جامعة محمد خضير بسكرة ، كلية الحقوق والعلوم السياسية ، الجزائر.

(2)القاضي, محمد عايد قفطان, (2014), القصد الجرمي في تزوير التوقيع الإلكتروني, رسالة ماجستير غير منشورة, جامعة جدارا, الأردن.

تناول القصد العام لهذه الجريمة, كأحد عناصر الركن المعنوي, بشق العلم؛ أي علم الجاني بأن يقوم بتزوير توقيع إلكتروني, بينما تناول الفصل الثالث من هذه الدراسة, القصد الخاص لجريمة تزوير التوقيع الإلكتروني, من حيث مضمونه, والباعث من إرتكابه, وهو استعمال التوقيع الإلكتروني المزور, فيما زور من أجله.

وتختلف الدراسة الحالية عن الدراسة السابقة في بيان طبيعة جريمة التزوير في التشريع الاردني والعراقي، وتختلف دراستنا الحالية عن الدراسة أعلاه بأن الباحث في هذه الدراسة قد ركز على موضوع القصد الجرمي في تزوير التوقيع الإلكتروني.

منهج الدراسة :

استخدم الباحث في هذه الدراسة المناهج التالية:

1- المنهج الوصفي التحليلي من خلال وصف بيانات وأركان وخصائص نصوص المواد المتعلقة بالتزوير في قانون العقوبات الاردني رقم 16 لسنة 1960، وقانون الجرائم الإلكترونية رقم 27 لسنة 2015و قانون المعاملات الإلكترونية الأردني رقم 15 لسنة 2015 وكذلك قوانين التشريعات المقارنة.

2- المنهج المقارن من خلال مقارنة النصوص القانونية التي وردت في القانون الأردني والقانونين التشريعية المقارنة.

الفصل الثاني

ماهية جريمة التزوير الإلكتروني

التزوير من الجرائم الدقيقة تحتاج في معالجتها عناية خاصة بسبب تباين طرائق التزوير وتطورها، حيث لم تقتصر جريمة التزوير بمفهومها التقليدي بل تطورت واصبح الان ما يسمى التزوير الالكتروني، وهذا الامر الذي دعا الدول المتقدمة إلى تناول جريمة التزوير في شكلها الجديد في قوانينها العقابية لاضفاء الحماية الجزائية على المعلومات او البيانات الموجودة في الشبكة الإلكترونية التي تتعلق بأثبات حقوق أو مراكز قانونية معينة[1].

وسيتناول الباحث بتقسيم هذا الفصل إلى مبحثين، نخصص في المبحث الأول مفهوم جريمة التزوير الالكتروني وتعريفه وخصائصه وطبيعته، ونخصص في المبحث الثاني الذي يتناول النموذج القانوني لجريمة التزوير الإلكتروني.

---

(1)عبيد ، دكتور رؤوف ، (2016) ، جرائم التزييف والتزوير ، الطبعة الثانية ، مكتبة الوفاء القانونية ، الاسكندرية ، ص121.

المبحث الاول

مفهوم جريمة التزوير الإلكتروني

تتميز جريمة التزوير الإلكتروني بمفهوم معين تميزها عن سواها من الجرائم الالكترونية التي يمكن أن ترتكب سواء بالطرق التقليدية او بالطرق الإلكترونية سواء بالحاسبات الآلية أوشبكات الاتصالات والانترنت[1].

ولذلك لابد من التعرف على مفهوم جريمة التزوير الإلكتروني، من خلال تعريف التزوير لغه وفقهاً وقانوناً ، للوصول الى مفهوم التزوير، والتعرف على كل ما يحيط به بشكل دقيق وبيان خصائصه و طبيعته وهذا ما سيتناوله الباحث في المطلب الأول، أما المطلب الثاني فسيتناول الباحث فيه الصيغ التشريعية لتحديد مفهوم جريمة التزوير الإلكتروني.

المطلب الاول

تعريف جريمة التزوير الإلكتروني وبيان خصائصها وطبيعتها

قبل التطرق في جريمة التزوير لابد من تعريف الجريمة في لغة و فقهاً و قانوناً وكذلك معرفة الجريمة الإلكترونية التي لها صلة في موضوع دراستنا لأن جريمة التزوير الإلكتروني تتصل بكل ما يخص الحاسوب ولواحقه.

---

(1)العبادي ، محمد حميد الرصفان ، (2015) ، الجرائم المستحدثة في ظل العولمة ، الطبعة الاولى ، دار جليس الزمان ، عمان ، ص177.

ولهذا قسم الباحث هذا المطلب إلى ثلاث فروع يحث خصص في الفرع الأول عن تعريف التزوير الإلكتروني ، وخصص في الفرع الثاني عن خصائص التزوير الإلكتروني ، إما الفرع الثالث خصص لطبيعة جريمة التزور الإلكتروني.

الفرع الأول: تعريف التزوير الإلكتروني :

تعتبر جريمة التزوير الإلكتروني احدى الجرائم الإلكترونية و أكثرها تعقيداً و أتصالها بالثقة العامة لذلك سوف يتطرق الباحث لتعريف التزوير لغة و وقانوناً وفقهاً وعلى النحو التالي [1]:

1- التزوير لغة : هو الزور والباطل والكذب والتقليد والمحاكاة والبعد عن الحق ، وهو ايظاً لفظ مشتق من كلمة مزور وهو الكذب والتلفيق وإدخال الباطل،وهو معنى واسع شامل لكل صنوف الغش والتحايل[2].

2-التزوير فقهاً : إن التزوير هو عملية مادية وصورة من صور الكذب التي يقوم بها شخص بغرض تغيير الحقيقة في محرر أو سند عمومي أو سند رسمي بأحدى الطرق المحددة في قانون ، وشأنه إلحاق الضرر بالحقوق أو المراكز القانونية لأحد أو بعض أطراف السند أو المحرر محل الادعاء بالتزوير[3].

(1)زين الدين، بلال امين، (2008)،جرائم نظم المعالجة الالية للبيانات،الطبعة الاولى،دار الفكر الجامعى،الاسكندرية،ص334.
(2)زين الدين، بلال امين ، جرائم نظم المعالجة الالية للبيانات ، مرجع سابق ، ص334.
(3)سعد،عبد العزيز ،(2005)،جرائم التزوير وخيانة الأمانة واستعمال المزور ،الطبعة الاولى،دار هومة،الجزائر ،ص14.

3-التزوير قانوناً : عرف قانون العقوبات الأردني رقم 16 لسنة 1960 في المادة 260(بأن التزوير هو تحريف مفتعل للحقيقة في الوقائع والبينات التي يراد اثباتها بصك او مخطوط يحتج بهما أو يمكن أن ينجم عنه ضرر مادي أو معنوي أو اجتماعي) [1].

وعرف القانون العقوبات العراقي رقم111 لسنة 1969 في المادة 286 (هو تغيير الحقيقة بقصد الغش في سند أو وثيقة أو أي محرر أخر بإحدى الطرق المادية أو المعنوية التي بينها القانون تغييرا من شأنه إحداث ضرر بالمصلحة العامة أو بشخص من الأشخاص)[2].

4-التزوير الإلكتروني : إن التزوير الإلكتروني هو تغيير الحقيقة يرد على مخرجات الحاسوب الآلي سواء تمثلت في مخرجات ورقية مكتوبة كتلك التي تتم عن طريق الطابعة، أو كانت مرسومة عن طريق رسم[3].

كما عرف الباحث التزوير الإلكتروني على أنه" تغيير الحقيقة في المحررات الإلكترونية بأي وسيلة وذلك بغية استعمالها.

الفرع الثاني : خصائص جريمة التزوير الإلكتروني :

جريمة تزوير الإلكتروني هو نوع من الجرائم الإلكترونية، وهي من أخطر هذه الجرائم خاصة إذا تعلق الأمر بتزوير محررات رسمية تمت على يد موظف مكلف بتحريرها مثل العقود، أو وثيقة إدارية تخص جهة حكومية لأن ذلك يمس بالثقة العامة في مثل هذه الوثائق[4].

---

(1)قانون العقوبات الأردني رقم 16 لسنة 1960، المادة (260).

(2)قانون العقوبات العراقي رقم 111 لسنة 1969 المادة (286).

(3)حجازي،عبد الفتاح بيومي،الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنيت ، مرجع سابق ، ص170.

(4)قهوجي،علي عبد القادر،(1992)،الحماية الجنائية لبرامج الحاسوب،بحث منشورمجلة الحقوق للبحوث القانونية والأقتصادية،كلية الحقوق،جامعة الأسكندرية،ص63

وذلك يتميز التزوير الإلكتروني بمجموعة من خصائص نوردها فيما يلي :

1- إمكانية إرتكاب جريمة التزوير في أي من مراحل تشغيل النظام :

يمكن ارتكاب جريمة التزوير في أية مرحلة من مراحل تشغيل نظام المعالجة الآلية وهي مرحلة الإدخال، المعالجة،الإخراج، ففي مرحلة الإدخال حيث تترجم المعلومات إلى لغة مفهومة من قبل الآلة يسهل إدخل معلومات غير صحيحة أو عدم إدخال الوثائق الأساسية والمعلومات المطلوبة[1] ، لذلك يمكن تصور التزوير المعنوي بإدخال معلومات غير صحيحة للإعتداد بها على أنها معلومات صحيحة، أو ترك إدخال معلومات أساسية وذلك من أجل تغييرالحقيقة ، كقيام موظف بإدراج أسماء أشخاص غير موجودين حقيقة[2].

أما في مرحلة المعالجة فيمكن إدخال تعديلات على برامج الحاسب الآلي لتحقق الهدف الإجرامي عن طريق التلاعب في برامج النظام المعلومات،كما يمكن تغيير النتائج عند مرحلة الإخراج بعد أن تم ادخال المعطيات ومعالجتها بطريقة صحيحة، بالدخول إلى نظام المعالجة الآلية من أجل تزييف الحقيقة، مثل قيام أحد الطلبة بالدخول إلى النظام المعلوماتي للكلية لتعديل نقاطه[3].

2- عدم وجود أثر مادي للتزوير الإلكتروني :

يتميز التزوير في المحرر الإلكتروني بعدم ترك أثر مادي على المحرر المزور كما هو الحال في المحرر الورقي ، حيث قد تظهر آثار التغيير بالإضافة أو الحذف باستخدام أدوات أو مواد

---

(1)شكري ، عادل يوسف عبد النبي ،(2008)،الجريمة المعلوماتية وأزمة الشرعية الجزائية ، مجلة الجريمة المعلوماتية ، عدد 7 ،ص 115.

(2)حنان ، براهمي ،جريمة تزوير الوثيقة الرسمية الإدراية ذات الطبيعة المعلوماتية ، مرجع سابق ، ص193.

(3)شكري ، عادل يوسف عبد النبي ، الجريمة المعلوماتية وأزمة الشرعية الجزائية ، مرجع سابق ، ص115.

كيميائية ، بينما لا تظهرهذه الآثار في النوع الأول حيث تتم الجريمة من خلال الوصول إلى المعلومات وتغيير مضمونها ، فهي جريمة فنية غير ملموسة[1].

3- تفرد شخصية المجرم ودوافعه :

ترتكب جريمة التزوير الإكتروني بوسائل تقنية ، ولذلك يحتاج مرتكبها إلى خبرة وتخصص في المجال الإلكتروني لأنه سيتعامل مع جهاز الكمبيوتر ونظام المعالجة الآلية للبيانات ، فقد يكون هذا المجرم الإلكتروني من الموظفين المتخصصين في مجال الحاسب الآلي ، وهم يحتلون المرتبة الأولى بين مجرمي المعلوماتية ، أو من القراصنة أو المخترقين وهم أشخاص يستغلون الحاسب الآلي ولكن بشكل غير قانوني ، وهم فئتين الهاكرز القراصنة الهواة، والكراكرز وهم القراصنة المحترفون[2].

ولكن قد تقع هذه الجرائم بدافع معنوي من أجل المتعة الشخصية والهو و إثبات القدرات والبطش في عالم الحاسوب الإفتراضي ، ومن ذلك ما قامت به عصابة "هاكرز" مكونة من خمسة أشخاص بالاستيلاء على أموال من حسابات بطاقات بنكية ، وقد كان من بينهم فرنسي قام بتزوير بطاقات الصراف الآلي واستعمالها في سحب مبالغ مالية، ثم إعادتها للبنك مجددا ليؤكد أن نظا م الحماية الذي يوفره البنك لهذه البطاقات ضعيف ويمكن اختراقه[3].

تعتبر جريمة التزوير الإلكتروني من الجرائم التي يخطط لها بخبرة أشخاص ذوي مهارة فنية عالية وخبرة وذكاء، وهي ذات طابع ذهني علمي تعتمد على المعلومات والمعارف الفنية

---

(1)السراني, عبدالله بن سعود محمد, فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني ، مرجع سابق ، ص66.

(2)أسامة سمير حسين ،(2011)،الإحتيال الإلكتروني الوجه القبيح للتكنولوجيا ،الطبعة الأولى ، الجنادرية للتوزيع ،الأردن ، عمان ،ص96.

(3)أسامة سمير حسين ، الإحتيال الإلكتروني الوجه القبيح للتنولوجيا ، مرجع سابق ، ص101.

والتكنولوجية التي فرضها التقدم العلمي والحضاري ، بتالي اذا وقعت جريمة التزوير بالخطاء او بالصدفة لا يمكن تصور وجود عقوبة لها إلا إذا ترتكب عمدية ، لان قد يسهوا بعض الموظفين عن تسجيل امر معين دون قصد .

الفرع الثالث : طبيعة جريمة التزوير الإلكتروني :

تطورت وتكاثرت العمليات الإلكترونية كأثر مترتب على الثورة الإلكترونية في المعاملات الإلكترونية ، و أهم ما يميز هذه العمليات الإلكترونية أنها تدور في فلك شبكة الإنترنت ، وبذلك فهي تستفيد من التقنيات التكنولوجية العاليه الخاصة بها في التعامل بين الأطراف مهما كانت طبيعتهم.

ومع ذلك فقد بدأت تظهر الأثار السلبية للثورة المعلوماتية في جرائم الإلكترونية التي ترتكب عن طريق وسائل التقنيه الحديثة ، وهي ما يطلق عليها الجرائم الإلكترونية ، خاصة و أن ارتكبت الجريمة عن طريق الحاسب الآلي و الإنترنت[1].

ومن هذه الجرائم على سبيل المثال جريمة إختراق النظم الأمنية لحماية البيانات المخزونة ضمن أنظمة الوسائل الإلكترونية ، وذلك بالاطلاع على هذه البيانات بطرق غير مشروعة أو بتخريب و إتلاف برمجيات حماية البيانات أو بالنسخ غير المشروع لها ، أو بسرقة وقت الحاسبات

(1)حجازي ، عبد الفتاح بيومي ،(2007)،مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنيت ، دار الكتب القانونية ، المحلة الكبرى ، مصر ، ص19.

وسرقة المعلومات ، أو بالتزوير البيانات و المعلومات ، أو بانتهاك حرمة الحياة الخاصة للأفراد[1].

وكما لاحظ جانب من الفقه بإن الجريمة الإلكترونية التي تقع على العمليات الإلكترونية قد تأثرت بالوسائل المستحدثة التي أوجدتها هذه الثورة ، بما يترتب عليه إنفراد هذه الجرائم بصفات خاصة تزيد من خطورتها ومن الآثار الضارة التي تترتب عليها[2].

ويبدو ذلك فيما يلي :

اولاً : إن التطور الذي حدث بسبب تكنولوجيا المعلومات قد تأثرت به كذلك وسائل الدفع النقدي التقليدية ، مما أدى إلى ظهور المستندات و والوثائق الدائنية ، وظهرت كذلك الوسائل الإلكترونية لتحل محل النقود و أوامر الصرف – الشيكات – وبدأت بطاقات الائتمان الداخلية محل النقود والشيكات[3] .

ثانياً : إنعكاس الثورة الرقمية التي فجرتها تكنولوجيا الاتصالات عن بعد على شكل ونوعية وأسلوب الجريمة المعاصرة والتي صاحبتها مستجدات غيرت من المفهوم التقليدي لعمليات التزوير ، وذلك بعد استخدام اليزر الرقمية الملونة وغير الملونة ، ودخول الحاسبات الآلية وما يرتبط بها من ماسحات وطابعات في ارتكاب التزوير في المستندات والعملات[4].

---

(1)حجازي ، عبد الفتاح بيومي ، (2004) ، التجارة الإلكترونية وحمايتها القانونية ، الطبعة الأولى ، دار الفكر الجامعي ، القاهرة ، ص14.

(2)علي محمود علي حموده،(2003) ،الادلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي ، بحث منشور ضمن أعمال مؤتمر الجوانب القانونية و الأمنية للعمليات الإلكترونية ، أكادمية شرطة دبي , المجلد الأول ، ص197.

(3)حجازي ، عبد الفتاح بيومي ، (2005)، جريمة غسل الأموال بين الوسائط الإلكترونية ونصوص التشريع،الطبعة الاولى،دار الفكر الجامعي،الإسكندرية، ص6.

(4)د.فخري،محمد صالح عثمان ، (1995) ، جرائم بطاقة الائتمان،الطبعة الأولى ، دار الشروق ،القاهرة ، ص6 .

وللأهمية القصوى لأجهزة الكمبيوتر الإلكترونية التي تعتمد عليها جميع الإدارات والمؤسسات والجهات المختلفة في القطاع العام والخاص لتدوين وتسجيل جميع النشاطات والأعمال والتعاملات الإدارية والمالية والتعاقدية والتجارية على شكل بيانات ومعلومات تخزن في ذاكرة الحاسبات الآلية ، وعلى شبكاتها، سواء كانت المعلومات عادية أو سرية ، وهذه تشكل أهدافاً ثمينة لمجرمي التزوير الإلكتروني، سواء كانت المسجلة على الأشرطة الممغنطة أو الاسطوانات المخزنة في ذاكرة الحاسب الآلي ، لهذا فأي تغيير يحصل يعتبر حكماً جريمة تزوير إلكتروني.

وفي حال تغيير البيانات والمعلومات المخزنة في الحاسب الآلي أو على شبكة الانترنت تعرف بجريمة التزوير الإلكتروني ، والتزوير بها يتم لأهداف غير مشروعة وسيتم استخدامها ليتحقق في ذلك جريمتين وهي جريمة التزوير وجريمة إستخدام التزوير.

ويمكن حصول التزوير بالوثائق بإدخال التغيير على المحرر بالإضافة أو الحذف أو الإضافة لبعض نصوصه ، أو وضع توقيع أو ختم مزور على الوثيقة أو أي تصرف يخالف الحقيقة بإدخاله في المحرر المراد تزويره، وتغيير الحقيقة قد يتم باستبدال اسم صاحب الوثيقة باسم آخر أو التزوير بالشيكات وقد يكون التزوير جزئياً أو كلياً[1].

أما المصلحة المحمية في جريمة التزوير الإلكتروني هي الثقة العامة في المحررات ذات القيمة القانونية اياً كان شكلها، وأن جريمة التزوير الإلكتروني ليست جريمة تقع على المحررات المعالجة الياً فقط ، بل تقع على المحررات الإلكترونية واستعمالها سواء كانت هذه المحررات رسمية أم غير رسمية.

---

(1)العبادي ، محمد حميد الرصفان ، الجرائم المستحدثة في ظل العولمة ، مرجع سابق ، ص178.

المطلب الثاني

الصيغ التشريعية لتحديد مفهوم جريمة التزوير الإلكتروني

هناك عدة صيغ تشريعية لتحديد مفهوم جريمة التزوير الإلكتروني بصفة عامة ومن أصنافها تزوير المحرر أو الوثيقة الإلكترونية ، ومن هذه الصيغ نجد صيغة نصوص قانون العقوبات الفرنسي كنموذج لتوسيع مفهوم التزوير في إطار نصوص قانون العقوبات ، أما صيغ بعض القوانين العربية – القانون المصري والإماراتي والإردني – نموذجاً على تحديد مفهوم التزوير الإلكتروني في قوانين خاصة أي مستقلة عن قانون العقوبات(1).

وقبل ذلك لابد من تطرق إلى مدى إمكانية إنطباق النصوص التقليدية الخاصة بالتزوير التقليدي على التزوير الإلكتروني ، و نبين أراء الفقهاء في هذا الموضوع.

وسيتناول الباحث في الفرع الأول عن مدى إمكانية انطباق نص التزوير التقليدي على التزوير الالكتروني، وسيتطرق أيضاً الباحث في الفرع الثاني عن صيغ التشريعية في إطار نصوص قانون العقوبات ، أما في الفرع الثالث فسيتناول الباحث عن الصيغ التشريعية للتزوير الإلكتروني بنصوص مستقلة (خاصة).

الفرع الأول : مدى إمكانية انطباق نص التزوير التقليدي على التزوير الالكتروني :

يتنازع مسألة انطباق نصوص تجريم التزوير في المحررات التقليدية على التزوير البيانات المخزنة في نظام الحاسوب، أو تزوير مخرجات الحاسوب لذلك هناك رأيين ، الرأي الأول وهو

---

(1)المحامي يونس عرب، (2002) ، جرائم الكمبيوتر والإنترنيت، ورقة عمل مقدمة إلى مؤتمر الأمن العربي ، تنظيم المركز العربي للدراسات والبحوث الجنائية ، ص436.

الرأي الراجح بفعل تبنيه من قطاع واسع من الفقه ، والمعزز ايضاً ببعض الأحكام القضائية ، وبفعل تم تبنيه في التشريعات الجزائية الحديثة في القانون المقارن يقوم على أن التزوير في معطيات الحاسوب ، لا يدخل تحت نطاق النصوص التقليدية(1).

أما الرأي الثاني ، فيرى إمكان تطبيق النصوص الجزائية المنظمة لجريمة التزوير التقليدية على الجرائم تزوير الإلكتروني. ووسوف نبين حجج اصحاب هذين الرأيين فيما يلي :

1- عدم إمكان تطبيق النصوص الجزائية التقليدية على جريمة التزوير الإلكتروني :

أبرز متبني هذه الاتجاه الفقيه Ulrich Seiber الذي يرى أن تزوير البيانات المخزنة الكترونياً، لا ينطوي تحت النصوص التقليدية ، لأن نصوص التزوير التقليدية في قوانين أكثر الدول، كأيطاليا والنمسا وسوسيرا وفرنسا وبلجيكا والمانيا (وطبعاً قوانين الدول المتأثرة بهذه القوانين كمصر والإمارات و العراق والأردن والدول العربية الأخرى) ، تفترض إمكانية القراءة البصرية لمحتويات المحرر المدونة فيه ، وهذا غير متحقق بالنسبة لمعطيات الحاسوب المخزنة وعزز رأيه هذا من خلال حقيقة أن المستقر في الفقه والقضاء أن الأسطوانة وشريط التسجيل، التي سجلت عليه العبارات أياً كانت أهميتها ، لا تعتبر محرراً ، ولا يعد تزويراً[2].

أما الفقيه Jaeger ، فيعزز هذا الرأي لديه ، أن البيانات ، سواء كانت مخزنة في ذاكرة الحاسوب أم منظمة في برامجة أو أشرطة الإدخال أو الأخراج الممغنطة ، فأنها ليست مقروءة بذاتها ، ولا يمكن للمعنى الذي تحمله أن ينتقل عن طريق العين البشرية ، إذ أنها تسجل على هيئة جزيئات دقيقة مجهزة ومثبته إلكترونياً على دعامة تتيح للحاسوب فقط قراءتها، مما ينفي عنها صفة

(1)المحامي يونس عرب ، جرائم الكمبيوتر والإنترنيت ، مرجع سابق ، ص435.

(2)المحامي يونس عرب ، جرائم الكمبيوتر والإنترنيت ، مرجع سابق ، ص436.

المحرر . كما أن المعالجة الإلكترونية التي يجريها الحاسوب ، وكذلك مخرجاته، لا تعبر عن فكرة بشرية ، وإنما تعبر عن فكرة ميكانيكية للآلة ، ويرد Jaeger على القائلين بإمكان دحض هذه الفكرة ، بالاستناد الى أن وراء كل آلة عقل بشري ، أن العقبة التي لا يمكن التغلب عليها ، والتي تمنع تطبيق نصوص التزوير التقليدية على التغيير أو التزوير الذي يقع في برامج الحاسوب أو البيانات المخزنة داخله ، إنما تكمن في وجوب حدوث تغيير في الحقيقة عن طريق الكتابة [(1)].

ولذلك يرى هذا الإتجاه عدم انطباق النص الجنائي الخاص بالتزوير في المحررات الرسمية أو العرفية الورقية على المحررات الإلكترونية لأنها ليست محرر بالمعنى القانوني.

وإن عدم امكانية تطبيق النصوص المتعلقة بالتزوير على تغيير الحقيقة في المعلومات المبرمجة لأنها لا تعتبر محرر من حيث أنه لا يمكن مشاهدة المعلومات المخزنة على وسائط التخزين الخاصة بها عن طريق النظر، وبالتالي فهي ليست مقروءة ولا يمكن للمعنى الذي تحمله أن ينتقل عن طريق العين المجرد.

ولذلك فإنه في إطار نص التزوير التقليدي لا يمكن مد هذا النص ليشمل التزوير في المحررات الإلكترونية لسببين:

أ- جمود النص الجزائي مما يصعب معه التأويل، لعدم وجود أي إشارة إلى الأشكال المستحدثة من المحررات ، طالما هناك ربط بين الوثيقة والكتابة التي لها مدلول ورقي غالباً.

---

(1)د. رستم، هشام محمد فريد ، (1995) ، قانون العقوبات ومخاطر تقنية المعلومات ، الطبعة الأولى ، مكتبة الآلات الكاتبة ، أسيوط ، ص328.

ب- التلازم بين قيام جريمة التزوير وشرط وجود محرر لها قيمة ثبوتية يقتضي الرجوع إلى قوانين الإثبات وكيفية تنظيمها للدليل المكتوب[1].

ولهذا يرى الباحث بإن هذه النصوص الخاصة بالتزوير التقليدي جامدة بحيث تربط الكتابة بالشكل الورقي ، و كذلك لا يمكن التوسع في تفسيرها و سيؤدي هذا بيغلق الباب أمام تفسير النص الجزائي، وبالتالي لا يمكن تطبيقه على المحررات الإلكترونية باعتبار أن مفهوم الكتابة لا يشملها.

2- إمكان تطبيق نصوص التزوير التقليدية على التزوير الإلكتروني :

يرى جانب من الفقه امكانية تطبيق نص التزوير القائم على فعل تزوير الإلكتروني، وهو ما حصل في فرنسا ، حيث أيد البعض فكرة تطبيق النص التقليدي لجريمة التزوير على كل تلاعب أو تغيير في المحرر الإلكتروني معتمدا في ذلك على التطبيق والتفسير القضائي ، ونصوص قانون الإثبات .

1- **التفسير القضائي الموسع لمعنى المحرر** : أصبح تفسير القضاء لمحرر تفسيراً موسعاً جدا كما هو الحال لدى القضاء الفرنسي، حيث يشمل كل محرر لها قيمة تصلح في الإثبات مهما كانت دعامتها ، وبما أن الواقع أصبح يفرض التعامل بالمحررات الإلكترونية ، فإن هذه المحررات قد تكون لها قيمة تصلح في الإثبات، إذا تم المحافظة على محتواها، وتحديد منشئها.

2- **تمتع المحرر الإلكترونية بقيمة ثبوتية بمقتضى قوانين الإثبات:** لقد أصبح المحرر الإلكتروني – خاصة تلك الصادرة عن الجهات الإدارية العامة– لها قيمة قانونية في الإثبات، ولما

---

(1)قورة ، نائلة عادل محمد فريد ،(2005)،جرائم الحاسب الآلي الإقتصادي ، الطبعة الأولى ، منشورات حلبي الحقوقية ، بيروت ، ص584.

كانت العلاقة قائمة بين جريمة التزوير وتمتع الوثيقة بهذه القيمة، أمكن مد النص الجنائي التقليدي ليشمل تزوير المحررات الإلكترونية[1].

ومن جهة أخرى فأن دلالة معطيات الحاسوب التقنية الواسعة والمفترض مراعتها في نطاق علاقتها بالقانون ، تشمل مخرجات الحاسوب شأنها شأن المدخلات أو البيانات محل المعالجة أو البرامج ويدعم هذا الرأي الفقه الفرنسي بعد صدور قانون 1988 الذي جرم تزوير المحررات المعالجة الياً واستعمال هذه المستندات قد إتجه إلى أن التغيير في الرموز وكلمات المستند المعالج الياً بعد استخراجه من الحاسوب تنطبق عليه النصوص التقليدية وليس النصوص القانون الجديد ، لأن التزوير في هذه الحالة قد تم على محرر ورقي يتمثل بمخرجات الحاسوب الورقية ، ولكن التزوير الإلكتروني هو الذي يكون التزوير الذي وقع بالاساس على البيانات داخل الحاسوب ولهذا لا يمكن أن نتصور هذا الرأي يمكن تطبيقه[2].

ولهذا أن نصوص التجريم التقليدية لجرائم التزوير، غير قابلة للإنطباق على جرائم التزوير الإلكتروني بدلالتها الواسعه ، وتعزز وتأيد هذا الإتجاه بأحكام قضائية في فرنسا وإمريكا وبريطانية وغيرها من النظم المقارنة ، لذلك لابد من تغيير في التشريعات التقليدية من أجل مواكبة مثل تلك الجرائم وخصوصاً في التشريعات العربية لمواجهة هذه الجرائم ، وصيانة الأسس ومبادئ النظانم القانوني وكفالة الحقوق التي تهددها هذه الإنشطة الجرمية المستجدة مع الأخذ بنظام الفرنسي الذي دمج القوانين الإلكترونية الخاصة بالتزوير الإلكتروني مع قانون العقوبات من أجل توحيد القوانين في قانون واحد .

---

(1)حنان ، براهمي ،جريمة تزوير الوثيقة الرسمية الإدراية ذات الطبيعة المعلوماتية ، مرجع سابق ، ص175.

(2)د. رستم، هشام محمد فريد،قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق ،ص 444.

الفرع الثاني : الصيغ التشريعية لتوسيع مفهوم التزوير الإلكتروني في إطار نصوص قانون العقوبات :

لقد اعتمدت بعض الدول نهجا معينا في تجريم التزوير الإلكتروني بصفة عامة، حيث تم توسيع نصوص قانون العقوبات ليشمل هذا النوع من التزوير، ومن هذه الدول نجد فرنسا، وذلك من خلال تعديل نصوص قانون العقوبات المتعلقة بالتزوير . لكن الإشكال يبقى قائماً بالنسبة للدول التي لم تعدل النصوص المتعلقة بالتزوير ، من حيث مدى إمكانية تطبيق هذه النصوص على هذا النوع المستجد من التزوير(1).

ولهذا تعتبر فرنسا نموذجا يقتدى به في دمج النصوص المستحدثة للجرائم الإلكترونية ومن ضمنها النصوص المتعلقة باجرائم التزوير الإلكتروني مع قانون العقوبات الفرنسي ولهذا ستتطرق الدراسة لها بلتفصيل.

وسع المشرع الجزائي الفرنسي في تجريم التزوير الإلكتروني ليمتد إلى المحرر أو الوثيقة الإلكترونية في القسم الأول ضمن الكتاب الرابع من قانون العقوبات تحت عنوان " الاعتداءات ضد الثقة العامة " في المادة 1/441 المعدلة في 14 ماي 1993.

وحيث تنص المادة 1/441 من القانون العقوبات الفرنسي على :

(1)حنان ، براهمي ،جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية ، مرجع سابق ، ص165.

"كل تغيير تدليسي للحقيقة يكون من طبيعته أن يسبب ضرر بأي وسيلة مهما كانت في محرر أو أي سند للتعبير عن الرأي والذي من ممكن أن يكون له الأثر في أنشاء دليل على حق أو فعل تكون له نتائج قانونية "[1].

يستنتج من النص السابق أن الوثيقة تشمل إلى جانب الشكل التقليدي لها– وثيقة ورقية – كل وسيط آخر سواء كان تقليدياً أو إلكترونياً للتعبير عن فكرة أو معاني معينة لكن يجب أن يكون لها قيمة قانونية لتصلح أن تكون ذات قيمة ثبوتية لإستخدامها كدليل إثبات حق أو واقعة لها آثار قانونية.

ولما كان التزوير هو تغيير للحقيقة في المحرر غشاً ، فقد أصبح للمحرر مفهوم أوسع في القانون العقوبات الفرنسي وهو التعبير المستخدم في النص السابق" أن يسبب ضرر بأي وسيلة مهما كانت في محرر أو أي سند للتعبير عن الرأي " وبل تحديد التعبير " بأي وسيلة " وبالتالي فقد شمل هذا المعنى كل الأشكال الحديثة التي نتجت عن استخدامات الإلكترونية والتي تحمل هذه الأفكار، ومن بينها الدعامات المادية مثل الاقراص الإلكترونية، أو البطاقات أو الشرائح المغناطيسية وغيرها ، ولا يكون التزوير معتبراً إلا إذا كان الوثيقة لها قيمة قانونية حيث أنها تثبت حقاً أو مركزاً قانونية ، أو يمكن استخدامها كدليل لإثبات واقعة قانونية[2].

واتجه البعض من الفقه للقول بان المشرع الفرنسي حقق في وضع هذا النص مكسبين، تمثل المكسب الأول بتوسيع الحماية القانونية على اعتبار أن أي نوع من أنواع التزوير سواء المادي أو الالكتروني يدخل ضمن الحماية المقررة ، وأما المكسب الثاني فهو لم يحدد طرق وقوع

(1)د. زين الدين ، بلال أمين ،جرائم نظم المعالجة الآلية للبيانات ،مرجع سابق، ص 331.

(2)حنان ، براهمي ،(2014)،جريمة تزوير الوثيقة الرسمية الإدراية ذات الطبيعة المعلوماتية ، مرجع سابق ، ص166.

التزوير على وجه الحصر كما فعل قانون أمن الشيكات والذي تناول التقليد والاصطناع وغيرها من الصور وإنما ترك ذلك بقوله بتحقق التغيير التدليسي بأي وسيلة كانت ، وعلى ذلك فالنص الجديد أوسع على اعتبار انه مرن ويستوعب أي حالة مستقبلية للتزوير [1].

إلا أن المشرع الفرنسي كان قد نظم الجرائم الإلكترونية بقانون خاص قبل التعديل في قانون العقوبات و المرقم 19/88 و المؤرخ في 5 يناير 1988، حيث نص في المادة 5/462 على :

"يعاقب بالحبس لمدة تتراوح من عام إلى خمسة أعوام وبغرامة يتراوح مقدارها من 20 إلى 2 مليون فرنك من قام بتزييف وثائق معلوماتية مهما كان شكلها أو طبيعتها وذلك للإضرار بالغير".

والمادة (6/462) : يعاقب بالحبس من عام إلى خمسة أعوام وبغرامة يتراوح مقدارها من 20ألف إلى 2 مليون فرنك أو بإحدى هاتين العقوبتين كل من قام عمدا باستخدام الوثائق المعلوماتية المشار إليها في المادة 5/462.

إن هذ النصوص تجرم تزوير الوثيقة المعالجة آليا مهما كان شكلها إذا سبب ذلك ضررا لغيير وكذلك عند أستعمال هذه الوثيقة.

وبالتالي فقد كان منهج المشرع الجزائي الفرنسي من خلال هذا القانون هو إفراد نص مستقل في قانون العقوبات لمواجهة تزوير الإلكتروني، و قد إعتبر الفقه الفرنسي هذه المواد مكملة

---

(1)حجازي ، عبد الفاتاح بيومي ، (2008) ، التزوير في جرائم الكمبيوتر والإنترنيت ، الطبعة الأولى ، دار الكتب القانونية ، مصر ، المحلى الكبرى ،ص 161 .

للمادة 150 الخاصة بتزوير المحررات[1]، وبذلك اعتبرت جريمة تزوير الوثائق الإلكترونية جريمة مستقلة عن جريمة التزوير في المحررات التقليدية[2].

لكن بعد تعديل قانون العقوبات الفرنسي لم يأخذ المشرع بالمادتين 5/462 و6/462 المتعلقتين بتزوير الوثيقة المعالجة آليا واستعمال الوثيقة المزورة باعتبار أن المادة 1/441 قد وسعت من مفهوم الوثيقة ، كما أن هذين المادتين لاقتا اعتراضات في مجلس الشيوخ عند مناقشة هذا القانون ، لما يترتب عليهما من مساواة بين المعطيات المعلوماتية بصفة عامة وبين المحررات من حيث القيمة القانونية[3].

لذلك غير المشرع الجنائي الفرنسي خطته بشأن تجريم تزوير المحررات الإلكتروني باعتبار أن المصلحة المحمية في جرائم المساس بالأنظمة الإلكترونية أو المعطيات والبيانات مختلفة عن تلك المتعلقة بجرائم التزوير في المحررات التي تتعلق بحماية الثقة العامة فيها . وبذلك اختفت جريمتا تزوير المستندات المعالجة آليا واستعمالها من الباب الثالث (المتعلق بالجرائم الإلكترونية) ، وأضافها إلى جريمة التزوير العادية بعد تطوير نصوصها بما يتلائم مع تلك المحررات[4].

---

(1)قورة ، نائلة عادل محمد فريد ،جرائم الحاسب الآلي الإقتصادي ، مرجع سابق ، ص587.

(2)شمس الدين ، أشرف توفيق ،(2006)،الحماية الجنائية للمستند الإلكتروني ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، ص108.

(3)قورة ، نائلة عادل محمد فريد ، جرائم الحاسب الآلي الإقتصادية ، مرجع سابق ، ص588 .

(4)القهوجي ، علي عبد القادر ، (2000) ، الحماية الجنائية للبيانات المعالجة إلكترونياً ، بحث مقدم إلى مؤتمر القانون والكمبيوتر و الإنترنت ، كلية الشريعة و القانون ، جامعة الإمارات العربية المتحدة ، ص41.

كما لم يحدد المشرع الفرنسي في المادة (441) طرق معينة لإرتكاب التزوير، وهذا يعني استخدام شتى الطرق والأساليب الإلكترونية أيا كانت لإرتكاب الفعل الإجرامي المتمثل في تزوير المستندات الإلكترونية[1].

لقد تطور القانون الفرنسي في مجال تجريم التزوير في المحررات الإلكترونية باعتباره من أخطر صور الغش في نطاق المعلوماتية بسبب خطورة الدور الذي يقوم به الحاسب الآلي في الوقت الحاضر وفي كل المجالات، فقد أصبحت تتم من خلاله عمليات هائلة ترتب آثار قانونية خطيرة[2].

بذلك حسم المشرع الجنائي الفرنسي الجدل الذي كان قائما من خلال المادة1/441 من قانون العقوبات، كما قطع كل خلاف حول مفهوم المحرر الذي أصبح ينصرف إلى الورقة المكتوبة والمحرر الإلكتروني التي عبر عنها بلفظ أي دعامة أخرى، حيث ينصرف هذا التعبير إلى كافة الأشكال المقررة التي يمكن أن تكون وعاء للتعبير عن فكرة أو يمكن أن ينتج عنها دليل على حق أو واقعة ذات آثار قانونية[3].

كما أخذ المشرع الفرنسي بمبدأ النظير الوظيفي الذي نص عليه قانون الأونسترال النموذجي وهذا المبدأ يعمل على تحليل دقيق لكل أغراض القواعد القانونية المنظمة للكتابة الورقية، ثم البحث عن كيفية تحقيق هذه الاغراض أو أداء تلك الوظائف عند استخدام الدعامات الحديثة.

وبتالي يعمل على المساواة بين المحررات الورقية و المحررات الإلكترونية في القيمة القانونية لها وحجيتها في الإثبات ، وهذه المساواة تأتي في عدة معايير موضوعية محددة، ثم

---

(1)زين الدين ، بلال أمين ، جرائم نظم المعالجة الآلية للبيانات ، مرجع سابق ، ص354.

(2)حجازي ، عبد الفتاح بيومي ، (2007)، الجريمة في عصر العولمة ، الطبعة الأولى، دار الفكر الجامعي ، الإسكندرية ، ص106.

(3)حجازي ، عبد الفتاح بيومي، التجارة الإلكترونية وحمايتها القانونية ، مرجع سابق ، ص165.

البحث في مدى امكانية أن تلبي هذه الدعامات الالكترونية تلك المعايير ، وإذا توافرت تلك المعايير في أي المستخرجات الالكترونية ، فإن المشرع يمنحها المستوى نفسه من الاعتراف أي انه يساوي بينها وبين المستندات الورقية التقليدية[1].

كما حقق المشرع الجنائي الفرنسي من خلال المادة 441 من قانون العقوبات هدفين: الهدف الأول : في استيعاب هذا النص حالات التزوير التقليدي في المحررات إلى جانب تزوير المحرر الإلكتروني ، وذلك بتجريم التزوير على المحررات الإلكترونية المطبوعة على سند أو دعامة مادية كشريط ممغنط أو قرص مدمج وبأي وسيلة.

الهدف الثاني : فهو خروج جريمتي تزوير المحررات المعالجة آليا واستعمالها ، من بين جرائم الإعتداء على نظم المعالجة الآلية للمعطيات[2].

الفرع الثالث : الصيغ التشريعية للتزوير الإلكتروني بنصوص مستقلة (خاصة):

لقد ساهمت الصعوبات التي واجهت تطبيق النص المتعلق بتجريم تزوير المحرر الورقي ليشمل المحررات الإلكترونية في ظهور اتجاه تشريعي يجرم تزوير هذه المحررات بنصوص خاصة نظرا لخصائص هذه الأخيرة التي تختلف عن الأولى، وأشكال التزوير الذي قد يقع عليها، مما جعل مفهوم التزوير الواقع على المحررات الإلكترونية يتحدد بحسب النص الجزائي الوارد في قانون مستقل.

---

(1)دليل التشريع قانون الأونسترال النوذجي للتجارة الإلكترونية لسنة 1996 ، ص20.

(2)المهيري ، خالد محمد كدفور، جرائم الكمبيوتر والإنترنيت والتجارة الإلكترونية ، الطبعة الثانية ، معهد القانون الدولي ، دبي ، ص645 وما بعدها .

من بين الإتجاهات التشريعية التي جرمت تزوير الإلكتروني بنصوص خاصة نجد بعض التشريعات العربية منها التشريع المصري، التشريع الإماراتي،والتشرع الأردني، حيث سنعرض كل تجربة على حدى، ثم نحاول استخلاص مفهوم تزوير الإلكتروني من خلال هذه النصوص.

1- صيغة التجريم في التشريع المصري من خلال قانون التوقيع الإلكتروني:

جرم المشرع المصري في قانون التوقيع الإلكتروني تزوير المحررات الإلكترونية بأشكاله المختلفة، وحيث نصت المادة 23 من قانون التوقيع الإلكتروني : " مع عدم الإخلال بأية عقوبة اشد منصوص عليها في قانون العقوبات أو في أي قانون آخر ، يعاقب بالحبس وبغرامة لاتقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين كل من :

- أتلف أو عيّب توقيعا أو وسيطا أو محررا الكترونيا ، أو زوّر شيئا من ذلك بطريق الاصطناع أو التعديل أو التحوير أو بأي طريق آخر .
- استعمل توقيعا أو وسيطا أو محررا الكترونيا معيبا أو مزورا مع علمه بذلك[1].

ولما كانت علة التجريم تتعلق بالثقة العامة في الوثائق عند تداولها بين الأفراد ، حيث تنتج هذه الثقة مما تتمتع به هذه الوثائق من قيمة قانونية عند الإثبات ، فإن التجريم يرتبط بمدى تمتع هذه الوثائق بتلك القيمة، ولذلك أضفى قانون التوقيع الإلكتروني على هذا التوقيع حجية في الإثبات في نطاق المعاملات الإلكترونية.

(1)قانون التوقيع الإلكتروني المصري ، رقم 15 ، سنة 2004 ، المادة (23).

وقد نصت المادة 18 من قانون التوقيع الإلكتروني شروط لابد توفرها في المحرر الإلكتروني وكذلك ضوابط فنية وتقنية لكي يضفا اليها قوة في الإثبات أو تقع ضمن الحماية القانونية وهذه الشروط في المادة (18):

- إرتباط التوقيع الإلكتروني بالموقع دون غيره .
- سيطرة الموقع دون غيره على الوسيط الإلكتروني.
- إمكانية كشف أي تعديل أو تبديل في بيانات المحرر الإلكتروني أو التوقيع الإلكتروني[(1)].

أما المادة 8 من اللائحة التنفيذية فقد بينت الضوابط الفنية والتقنية التالية :

- امكانية تحديد وقت وتاريخ إنشاء الوثيقة الإلكترونية الرسمية أو العرفية من الناحية الفنية، من خلال نظام حفظ الكتروني مستقل.
- تحديد منشئ الوثيقة الإلكترونية الرسمية أو العرفية ، ودرجة سيطرته على الوسائط المستخدمة في إنشائها.
- إذا كانت الوثيقة الإلكترونية أنشأت باستخدام نظام الأتمتة فلا بد من التحقق من وقت وتاريخ إنشائها[(2)].

رغم أن المشرع المصري جرم تزوير التوقيع أو المحرر الإلكتروني في قانون التوقيع الإلكتروني، بعد أن ضمن لهذا التوقيع أو المحرر القيمة القانونية اللازمة في الإثبات من خلال الضوابط الفنية والتقنية المشار إليها في نفس القانون، إلا أنه لم يحرص صياغة النص المجرم

(1)قانون التوقيع الإلكتروني المصري ، رقم 15 ، سنة 2004 ، المادة (18).

(2)الائحة التنفيذية ، الصادرة من وزير الأتصالات و تكنولوجية المعلومات لقانون المصري ، رقم القرار 109، سنة 2005 .

لهذا الفعل بشكل جيد حيث لم يبين أركان التزوير بدقة ، بل اكتفى بيان بعض صور السلوك المادي مثل التعديل والإصطناع .

كما أنه جمع بين جريمتي الإتلاف والتزوير رغم اختلافهما من حيث نتيجة السلوك المادي، وذلك ظاهر من خلال العبارات المستخدمة مثل أتلف ، عيب توقيعها أو وسيطا أو محررا الكترونيا. كما خلا النص تماما من ذكر عنصر الضرر في جريمة التزوير.

2-صيغة التجريم في التشريع الإماراتي من خلال القانون الإتحادي لجرائم تقنية المعلومات:

جرم المشرع الإماراتي في القانون الإتحادي الخاص بجرائم تقنية المعلومات بعض الأفعال التي تتصل بالأنظمة المعلوماتية أو باستخدام جهاز الكمبيوتر، ومن الأفعال المتعلقة باستخدام هذا الجهاز جرم المشرع الإماراتي في المادة (4) فعل التزوير في مستند من مستندات الحكومة الإتحادية أو المحلية أو المؤسسات العامة الإتحادية والمحلية المعترف بها قانونا في نظام معلوماتي،حيث شدد العقوبة في هذه الحالة وهي السجن المؤقت فيما تكون العقوبة الحبس والغرامة أو احدى هاتين العقوبتين إذا وقع التزوير في مستند غير صادر عن هذه الجهات[1].\

وقد نصت المادة 1/4 على : " يعاقب بالسجن المؤقت كل من زور مستنداً من مستندات الحكومة الإتحادية أو المحلية أو الهيئات أو المؤسسات العامة الإتحادية والمحلية معترفاً به قانوناً في نظام معلوماتي.

(1)قانون مكافحة جرائم تقنية المعلومات الإماراتي ، رقم 2006/2، والمؤرخ 30 يناير سنة ،2006 المادة (4).

وتكون العقوبة الحبس و الغرامة أو إحدى هاتين العقوبتين إذا وقع التزوير فيما عدا ذلك من المستندات إذا كان من شأن ذلك إحداث ضرر.

ولمكافحة إحدى أخطر هذه الجرائم شدد المشرع الإماراتي العقوبة عندما يتعلق الأمر بتزوير مستند حكومي ذو طبيعة معلوماتية بالمقارنة مع المستندات غير الحكومية لما لهذا المستند من أهمية باعتباره مستندا رسميا،وبالتالي الإعتداء عليه بالتزوير يزعزع الثقة التي يتمتع بها عند تداوله خاصة وأنه يتمتع بالحجية المطلقة في مجال الإثبات ، لذلك شدد المشرع الإمارات ي على ذلك لمكافحة مثل تلك الجرائم.

3- صيغة التجريم في التشريع الأردني من خلال قانون الجرائم الإلكترونية :

جرم المشرع الأردني في قانون الجرائم الإلكترونية رقم 27 لسنة 2015 الأفعال التي تتصل بالجرائم الإلكترونية وبأسخدام جهاز الكمبيوتر ، ومن الأفعال المتعلقة باستخدام هذا الجهاز جرم المشرع الأردني في المادة (4) [(1)] :

" يعاقب كل من أدخل أو نشر أو استخدم قصدا برنامجا عن طريق الشبكة المعلوماتية أو باستخدام نظام معلومات لإلغاء أو حذف أو اضافة أو تدمير أو افشاء أو اتلاف او حجب او تعديل او تغيير او نقل او نسخ او التقاط او تمكين الأخرين من الاطلاع على بيانات او معلومات او اعاقة او تشويش او ايقاف او تعطيل عمل نظام معلومات او الوصول إليه او تغيير موقع الكتروني او الغائه او اتلافه او تعديل محتوياته او اشغاله او انتحال صفة او انتحال شخصية مالكه دون تصريح بالحبس مدة لا تقل عن 3 شهور وبغرامة لا تقل عن 200 دينار ولا تزيد عن 1000 دينار".

---

(1)قانون الجرائم الإلكترونية الإردني، رقم 27 ، لسنة 2015 المادة (4).

وتصل بعض العقوبات الواردة في القانون الى الحبس مدة لا تقل عن 5 سنوات وغرامة مالية لا تقل عن 5 ألاف دينار ولا تزيد عن 15 إلف دينار.

وشدد القانون العقوبات على من يرسل او ينشر عن طريق نظام معلومات او الشبكة المعلوماتية قصدا كل ما هو مسموع او مقروء أو مرئي يتضمن اعمالا إباحية او تتعلق بالاستغلال الجنسي لمن لم يكمل الثامنة عشرة من عمره بالحبس لمدة لا تقل عن 3 شهور ولا تزيد عن سنة وبغرامة لا تقل عن 300 دينار ولا تزيد عن 5 آلاف دينار[1].

ويرى الباحث إن من المهم أن ننوه إلى مسألة غاية في الأهمية ألا وهي الطريقة التشريعية التي تعالج بها الجرائم الإلكترونية ، فالمتتبع لنهج المشرع الأردني والعراقي وكذلك نهج التشريعات العربية يرى أنه أتجه إلى تنظيم قوانين التي تعالج مشاكل قانونية مستحدثة بشكل مستقل ، كما هو الحال بالقوانين الجرائم الإلكترونية وبالخصوص جريمة التزوير الإلكتروني ، ولذلك أن فكرة تبني المعالجة المستقلة للجرائم الإلكترونية في قوانين جديدة هو أمر يحتاج لأعادة النظر فيه لسببين :

الأول : فيتمثل بالناحية التنظيمية فليس من الأفضل أن نعالج كل مجموعة من الجرائم بقانون منفرد لأنه يؤدي إلى أيجاد قوانين عقابية متعددة وبالتالي تنتفي الغاية الأساسية من قانون العقوبات الذي يرتكز على فكرة تجميع النصوص العقابية في متن واحد.

الثاني : يتمثل في أن وقوع التضارب أو التداخل بين النصوص هو من الأمور الواردة عند المعالجة بهذا الشكل وبالتالي نكون أمام مشاكل قانونية في غنى عنها ، ومن خلال ما تقدم يرى

---

(1)وكالة الانباء الاردنية ، قانون الجرائم الإلكترونية يغلظ العقوبات ويدخل حيز التنفيذ ، 2015/6/2 ، (http://petra.gov.jo/Public_News/Nws_NewsDetails.aspx?Site_Id=2&lang=1&NewsID=198652&CatID=13).

الباحث أنه من الأفضل أن يتم الاكتفاء بإدخال التعديلات في قانون العقوبات و أخذ نموذج يقتدى به وهو قانون العقوبات الفرنسي الذي عمل على ذلك ويتطور إلى هذه اللحظة وذلك من أجل الإبتعاد عن تلك المشاكل.

المبحث الثاني

النموذج القانوني لجريمة التزوير الإلكتروني

التزوير الإلكتروني شأنه شأن بقية الجرائم يتكون من ركنين هما الركن المادي والركن المعنوي يختلف عنهما من حيث أنه يشترط لتحقيقه أن يتوفر الركن ثالث خاص هو (الضرر) حتى يتم معاقبة فاعله [1]، سنعمل على تقسيم هذه الاركان على ثلاث مطالب، حيث يتناول الباحث في المطلب الأول الركن المادي لجريمة التزوير الإلكتروني، والمطلب الثاني الركن المعنوي لجريمة التزوير الإلكتروني ، والمطلب الثالث الركن الخاص لجريمة التزوير الإلكتروني.

المطلب الأول

الركن المادي لجريمة التزوير الإلكتروني

الركن المادي في جريمة التزوير يعني وقوع نشاط إجرامي من شأنه تغيير الحقيقة في محرر بطريقة ما ، نص عليه القانون وأن يكون من شأن هذا التغيير إلحاق الضرر بالغير أو احتمال حدوثه .

---

(1)حجازي ، عبد الفاتاح بيومي ، التزوير في جرائم الكمبيوتر والإنترنيت ، مرجع سابق ، ص 60.

فيشترط لقيام التزوير توفر ثلاث عناصر حيث العنصر الأول هو تغيير الحقيقة وهذا ما يبنه الباحث في الفرع الأول ، و كذلك العنصر الثاني هو وجود محرر وهذا ما يبنه الباحث في الفرع الثاني ، أما العنصر الثالث هو أن يتم التغيير بإحدى الطرق التي نص عليها القانون وسيتطرق له الباحث في الفرع الثالث.

الفرع الأول : تغيير الحقيقة :

تغيير الحقيقة هو الأساس الذي تقوم عليه جريمة التزوير، وإذا انتفى ذلك العنصر، فلا تقوم جريمة التزوير ، كأن يقوم أحدهم بإثبات بيانات مطابقة للحقيقة ، فلا تقوم جريمة التزوير حتى ولو كان ذلك الشخص يعتقد بعدم صحة هذه البيانات وحتى ولو ترتب على فعله ضرر في حق الغير[1] .

وتحريف الحقيقة هي الفعل الجرمي الذي يتحقق به التزوير ، فأذا انتفى تحريف الحقيقة انتفى التزوير . كما لا يتحقق التزوير اذا كانت البيانات التي قام بها الجاني لا تتعلق بالغير. وتترتب على ذلك النتائج التالية:

1- لا تعد الصورية تزويراً.

الصورية تعني تغيير الحقيقة في عقد باتفاق اطرافه، وتنطوي على اخفاء طبيعة العقد الذي تم الاتفاق عليه، وبعبارة اخرى فان الصورية تعني ان يبطن المعتاقدان في العقد المستتر غير ما يعلنانه في العقد الظاهر.

---

(1)د . فوزية ، عبد الستار ،(1988)،شرح قانون العقوبات ، القسم الخاص ، دار النهضة العربية ،القاهرة ،ص245.

فان كان العقد المستتر هو المعبر عن الإرادة الحقيقية للمتعاقدين فهو الذي يمثل الحقيقة ،لان العقد الظاهر يغاير الحقيقة التي يثبتها العقد الباطن.

2- لا يعد تحريف الحقيقة في الاقرارات او التصاريح الفردية تزويراً.

وهي ما يصدر من طرف واحد ، وبعبارة اخرى فهي مجموعة من البيانات التي يثبتها شخص في صك أو في مخطوط وتكون خاصة به وحده ولا تمس غيره

- كاقرارات التجار عن بضائعهم الصادرة أو الواردة إلى ادارة الجمارك .
- وكما لو ذكر شخص في صك أو مخطوط أو محرر أن له الحق دون أن يمس المركز القانوني لغيره .

3- لا يعد تغيير الذي يقوم به من له الحق في اثبات الواقعة تزويراً.

اجاز المشرع للمدعى عليه وحده اثبات البيانات التي تناولها التغيير بحيث لا يتضمن فعله نسبة بيانات الى الغير ،فأذا غير في البيانات وجعلها تحقق مصلحته فهو يدفع عدواناً على حقه[1].

والقانون لا يهتم بأي فعل يصدر عن شخص في أثناء تناوله لجريمة التزوير في المحررات ما لم ينتج عن هذا الفعل تغييرا للحقيقة ولو كان هذا التغيير بالطرق المادية أو المعنوية التي نص عليها القانون وحتى ولو كان الشخص يعتقد في كنانة نفسه بأن الفعل الذي قام به قد أحدث تغييرا لهذه الحقيقة، فلا يعد المتهم قد ارتكب جريمة التزوير في محرر بطريقة وضع إمضاءات مزورة إذا

---

(1)المشهداني ، محمد أحمد ،(2001)،شرح قانون العقوبات، القسم الخاص،الطبعة الأولى،عمان،ص372 وما بعدها.

قام بوضع هذا الإمضاء بناء على إذن من صاحب الشأن أو إذا قام بالإمساك بيد المريض طريح الفراش والذي لا يستطيع الحراك كي يوقع بيده على المحرر(1).

ويتصور وقوع التزوير الإلكتروني عن طريق تغيير الحقيقة على شرائط أو المحررات التي تمثل مخرجات الحاسب الآلي أي لابد أن يحصل التغيير في البيانات الموجودة في جهاز ، شرط حصول ضرر والذي يتمثل في اهتزاز الثقة المفترضة في المحررات الرسمية حال التزوير الإلكتروني في المحرر الرسمي أو يلحق لأحد الأفراد وذلك حال التزوير الإلكتروني في المحرر العرفي.

ولكن أذا كان جوهر التزوير هو تغيير الحقيقة في محرر ، كما هو في قانون العقوبات الأردني والعراقي ، أو كما يطلق عليه قانون العقوبات الفرنسي بأنه التغيير التدليسي للحقيقة في المادة 1/441 ، فأن السؤال ما هو مدلول تغيير الحقيقة ، وبمعنى آخر ماهو مفهوم هذا التغيير للحقيقة والذي إن وجد يعد تزويراً ؟

فتغيير الحقيقة يجد نطاقه في أنه استبدال للحقيقة بما يخالفها ، بمعنى إدخال تغيير على المحرر المراد تزويره على نحو يغيير مضمونه أو شكله ولكن بشكل لا يعدمه أو يهدر قيمته ، ومثاله من يحذف اسم صاحب الشهادة الحصول على درجة علمية وبدون اسمه بدلا عنه ، أو من يحذف اسم المستفيد من شيك يعثر عليه وبدون اسمه هو ليصبح المستفيد .

ويقصد في تغيير الحقيقة كذلك ، ليس تغيير الواقعه المطلقه ، إنما الحقيقة النسبية كأن يثبت في المحرر المزور ما يخالف إرادة صاحب الشأن حتى ولو صادف ذلك الواقع فعلا ، كما ينصرف التغيير كذلك إلى حقيقة الثانية التي يقترحها المشرع ، أي البيانات التي حددها القانون

---

(1)زين الدين ، بلال أمين ، جرائم نظم المعالجة الآلية للبيانات ، مرجع سابق ، ص337.

والتي بتمامها يعيد للمحرر قوته القانونية ، ففي هذا الفرض تتوافر الحقيقة القانونية التي وإن تغيرت يكون التزوير قد وقع في شأن حقيقة قانونية افترضها المشرع[1] .

ومما تجدر الأشارة إليه أن التزوير الإلكتروني لا يتم من قبل مشغل الحاسب الآلي فحسب، وإنما يمكن ان يقع من شخص عادي ليس له أي دراية بتشغيل الكمبيوتر ولا يتمتع بأي قدر من الكفاءات و المهارات الفنية والعلمية لتشغيل هذا الجهاز الإلكتروني ومع ذلك يرتكب التزوير الإلكتروني كما هو الحال بالنسبة للشخص الذي يعمد إلى فتح حساب جاري فيقوم باستعمال اسم شخص آخر أو الانصاف بصفة ليست له،أو بتقرير وقائع كاذبة أو أي أمر من شأن المستند المبرمج إثباته.

كما ويتم تغيير الحقيقة بنشاط إيجابي فأنه يتحقق بنشاط سلبي ألا وهو الترك ، وذلك إذا ترتب على الترك تغييراً جوهرياً سبب ضررا للغير لأن الترك يعتبر تغييرا للحقيقة ، وبتالي يعد تزويراً الإلكترونيا لاسيما إذا كان الترك متعمداً وليس على سبيل الخطأ أو السهو[2].

وعليه فإن تغيير الحقيقة كعنصر من عناصر الركن المادي لجريمة التزوير الإلكتروني تقع على البيانات والمعلومات بأي لغه كانت و بأي طريقة وجدت ، حيث لا يهم المادة التي كانت عليها و لايهم شكلها سواء كانت صوراً أم رموزاً أم علامات ، ويستوي أن يكون التغير مادياً أو معنوياً ، إذ لم يشترط في تغيير الحقيقة التقليدية أن تكون بطريقة معينة فإنه يشترط في تغيير

(1)د. فوزية ، عبد الستار ،شرح قانون العقوبات ، القسم الخاص ،مرجع سابق ،ص246.

(2)حجازي ، عبد الفتاح بيومي ،(2002)،التجارة الإلكترونية وحمايتها الجنائية،دار الفكر الجامعي،الإسكندرية،ص50.

الحقيقة التزوير الإلكتروني أن تتم باستخدام الحاسب الآلي لغرض تمييزها عن جريمة التزوير التقليدية[1] .

الفرع الثاني : وجود محرر :

تغيير الحقيقة موضوع جريمة التزوير هو الذي يكون محله محررا، والمحرر في مضمونه الكتابة مركبة من حروف أو علامات تدل على معنى أو فكرة معينة ، إمكانية القراءة البصرية لمحتواه و هو ما تفترضه نصوص التزوير التقليدية في أكثر الدول وحسبما حددها الفقه والقضاء[2].

ولا أهمية لنوع المحرر ، فالتزوير قد يقع على عقد أو على سند ، أو مخالصة أو خطاب أو برقية أو حكم أو تذكرة قطار أو سهم أو دفتر تجاري أو محررات إلكترونية وغيرها ... الخ.

وينبغي أن يقع تغيير الحقيقة في كتابة المحرر أي في عباراته أو فيما عليه من تأشيرات و علامات مختلفة ، أما التغيير فيما عدا ذلك فلا يعد تزويراً ، ولذا حكم بانتفاء التزوير في وضع صورة شخصية على رخصة رسمية بدلاً من صورة صاحبها الأصلي دون أي تغيير آخر ، لأن الصورة الشمسية ليست جزءاً من المحرر ولا تعد نوعاً من الكتابة المعروفة[3].

والمحرر الإلكتروني يختلف كلياً في شكله عن الشكل التقليدي العرفي أو الرسمي بل اضيف اليه محررات و وثائق جديدة الشكل وكذلك طريقة معينة لتدوين البيانات والمعلومات عليها،

---

(1)الحكيمي ، عبد الباسط محمد سيف ، (2000) ، النظرية العامة للجرئم ذات الخط العام اطروحة لنيل شهادة دكتوراه ، بغداد ، ص68.

(2)د. رستم، هشام محمد فريد ، قانون العقوبات ومخاطر تقنية المعلوماتمرجع سابق ، ص326.

(3)د. رؤوف عبيد ، جرائم التزييف والتزوير ،مرجع سابق ص134 وما بعدها.

التي طغت على الجانب والشكل التقليدي حتى شملت كافة الأنشطة والمجالات التي تتعلق بالنظم الإلكترونية وأصبح لها قيمة قانونية يعتمد عليها في الإثبات.

ويتسم المحرر بثلاث سمات ولابد من توفرها لكي يصبح المحرر ضمن الحماية القانونية :

1- أن يتخذ المحرر شكلاً كتابياً :

طالما هو محرر فيجب أن يكون مكتوباً وبأي لغة فقد تكون لغة محلية أو أجنبية وقد ذهب البعض إلى أنه يجب أن تكون الكتابة عبارة عن حروف والراجح أن يكون علامات اصطلاحية محل أتفاق، ويجب إدراك مضمون المحرر بالنظر إليه أو لمسه وإذا استحال قرائته فلا يصلح وسيلة للإثبات ولا عقاب على ما احتواه ولا عبرة بالمادة التي سطرت عليها الكتابة فقد تكون ورقة أو خشب أو جلد.

2- أن تكون الكتابة منسوبة لشخص معين :

يجب أن يكون المحرر منسوباً لأحد الأشخاص فيكون معروفاً أو يمكن معرفته وكل شك حول معرفته يسلب المحرر مظهره القانوني وقوته في الإثبات.

3- أن يحدث المحرر أثراً قانونياً :

يجب أن يتضمن المحرر موضوع جريمة التزوير تعبيراً عن الإرادة أو إثبات للحقيقة فإن لم تكن الكتابة صالحة لإحداث أثر قانوني كاستبدالها بغيرها أو تحريفها أو اصطناعها لا يعد تزويراً فالحماية القانونية تنصب على المصالح أو المراكز القانونية المرتبطة بهذا المحرر [1].

---

(1)د.عفيفي ، كامل عفيفي ، (2007) ، جرائم الكمبيوتر وحقوق الؤلف والمصنفات الفنية ودور الشرطة والقانون ، الطبعة الثانية ، منشورات الحلبي الحقوقية ، بيروت ، ص243.

والمحررات في بيئة الحاسب الآلي بيانات ومعلومات ذات معنى لا تدركها الحواس إن أمكن معرفتها وإدراك محتواها ، وهي ذات صيغة معنوية ، ولكن طالما إن المحرر الإلكتروني تم المشرع على الإعتراف به واعطاه الصبغة والحماية القانونية فأي اعتداء عليه بل تغيير يعتبر تزويراً يعاقب عليه القانون.

الفرع الثالث : طرق التزوير وعلاقتها بالتزوير الإلكتروني:

هناك عدة طرق للتزوير الإلكتروني وهي طرق تزوير مادي وطرق تزوير معنوي لذلك سوف نبينها في النقاط التالية مع بيان علاقتها بالتزوير الإلكتروني :

اولاً : طرق التزوير المادي :

1-وضع إمضاءات أختام أو بصمات مزورة :

وذلك بان ينسب المحرر المزور إلى شخص لم يصدر عنه ، ذلك إن ظهور إمضاء شخص أو ختمه أو بصمته في محرر يعني أن ما يتضمنه قد يصدر عنه ، إذ الإمضاء وما في حكمه هو رمز الشخصية ودليلها.

ويكون الإمضاء مزوراً متى وضع الجاني إمضاء شخص آخر في المحرر ، أو بتغيير آخر "يضع إمضاء ليست له في محرر" ، ويكتفي المشرع في ذلك بوضع الإمضاء ولا يتطلب تقليده.

ويترتب على اعتبار الإمضاء مزوراً ، أن وضع الإمضاء في المحرر لم يكن تعبيراً عن إرادة صحيحة لمن ينسب إليه المحرر ، ومع ذلك ينسب إليه المحرر.

مثال ذلك أن يوقع شخص على محرر باسم العائلة بعد أن يضيف إلى الاسم العائلي اسم شخص آخر بهدف أن ينسب إليه هذا المحرر[1] .

أما الختم المزور فيكون بوضع ختم لشخص على محرر، وهدفه نسبه المحرر لصاحب الختم مع أن إرادة ذلك الشخص لم تتصرف إلى ذلك ، سواء قلد ختماً لذلك الشخص واستعمله أو استحصل على ختمه الحقيقي ووقع المحرر به ، فالتزوير قائم حتى ولو كان الختم صحيحاً [2].

أما عن إمكانية وقوع التزوير الإلكتروني بهذه الطريقة فهو أمر وارد إذ ما تأملنا طبيعة وظيفة جهاز الحاسب الآلي وشبكة الإلكترونية التي ترتبط بها هذه الحواسب سواء كانت نظم معلومات داخلية أو شبكة المعلومات العالمية.

فمن المعلوم أن جهاز الحاسب الآلي ، أياً كان الموقع و أياً كانت المنظمة الإدارية التي يخدم فيها ، يتلقي بيانات يغذى عليها نظامه المعلوماتي وهي المدخلات ، وهذه المدخلات تعكس العمليات و الأنشطة التي تجري داخل المنظمة الإدارية سواء كانت مؤسسة صناعية أو شركة تجارية أو وزارة ، وهذه البيانات و المعلومات التي تتعلق بطبيعة نشاط الجهة كعدد العملاء المتعاملين معها وأصناف البضاعة و أسعارها ، أو نشاط الوزارة ، والخطط التي تنفذها إلى آخره ، وهذه المدخلات يقابلها ما يسمى بالمخرجات ، وهي أمور تحتاجها المنظمة أو الجهة كي تصدر قرارها في الوقت المناسب ، وما بين عملية (الإدخال و الإخراج) يقوم الحاسب الآلي بعملية تحليل البيانات ومعالجتها ، للوصول إلى مخرجات الحاسب الآلي تحتاجها الإدارة [3].

---

(1)حسني ، محمود نجيب ، شرح قانون العقوبات ، القسم الخاص ، مرجع سابق ، ص230.

(2)مجموعة أحكام النقض ،س 6 ، رقم445 ، ص579 .

(3)حسبو ، أحمد عمرو ،(2000)،حماية الحريات في مواجهة نظم المعلومات ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، ص 39 .

وطالما أن المتداول في جهاز الحاسب الآلي عبارة عن معلومة ، وهذه المعلومات ذات قيمة في ترتيب حق معين أو أثر قانوني معين فمن السهل تزوير مخرجات الحاسب المتضمنة هذه المعلومات [1].

فهذه المخرجات قد تتمثل في قرار إداري من جهة حكومية يرتب أثراً قانونياً معيناً ، ويكون ذلك القرار ممهوراً بتوقيع الوزير أو الرئيس الإداري الأعلى في الجهة مصدرة القرار ، ومن سهل إدخال صورة توقيع الشخص المنسوب إليه التزوير عن طريق جهاز الماسح الضوئي المرتبط بالحاسب الآلي ، ويضاف التوقيع للورقة التي انطوت على بيان المزور ، وبذلك تكون قد اكتسبت صفتها الرسمية بعد أن تنصرف إرادته إلى ذلك ، وما يصدق على التوقيع يصدق كذلك على " نموذج البصمة " وكذلك "الختم الشخصي" إذ يمكن الحصول على نسخه لهما إدخالهما على المستند المدعي نسبته لصاحب البصمة والختم ، وبذلك يمكن الحصول على المستند صحيح من ناحية الشكلية ولكنه مزور بالنظر إلى أنه نسب إلى شخص بعد أن حمل إمضائه أو ختمه على غير إرادته شرط إعتراف المشرع بالمخرجات المترتبة على عمليات الكمبيوتر في الإثبات الجزائي أو المدني[2].

والأصل في ذلك أن ما يتداول في الحاسب الآلي هو معلومة وهذه المعلومة ذات قيمة اقتصادية أو ثقافية وطالما أصبحت المعلومة ذات قيمة فمن الممكن سرقتها وبالتالي يمكن تزويرها.

---

(1)حجازي ، عبد الفتاح بيومي ، تزوير في جرائم الكمبيوتر والإنترنيت ، مرجع سابق ، ص206.

(2)حسبو ، عمرو أحمد ، حماية الحريات في مواجهة نظم المعلومات، مرجع سابق ، ص 30 .

وقد شهد التطبيق العملي لنشاط الحاسب الآلي حالات تزوير مضمونها إبرام صفقات وهمية بأسماء أشخاص آخرين أو الحجز الوهمي لأماكن في وسائل النقل والفنادق أو طلب شراء سلع أو خدمات بأسماء أشخاص مزورة [1].

2- تغيير المحررات أو الأختام أو الإمضاءات أو زيادة الكلمات :

ويقصد بهذه الطريقة ، كل ما يمكن إدخاله من تغيير مادي لصلب المحرر أو الإمضاء أو الختم الموضوع عليه ، وذلك لإحداث تعديل في معناه ، ويدخل ضمن هذه الطريقة ، زيادة كلمات على محرر [2].

ويشترط أن يقع التغيير بالحذف أو بالإضافة أو بالتعديل ، بعد إتمام المحرر ، أما التغيير الحاصل أثناء التحرير فهو تزوير معنوي لا مادي . ويشترط كذلك أن يقع التغيير بغير علم ذوي الشأن ولا موافقتهم ، إلا فلا تزوير ، كاتفاق المتعاقدين على زيادة عبارات في عقد عرفي أو على حذف شيء منها ، ولو بعد تحريره والتوقيع عليه منهما [3] .

وتحدث الإضافة بزيادة كلمة إلى اسم ورد في المحرر أو إلى الإمضاء أو بزيادة رقم لمبلغ الموجود أو المكتوب في المحرر أو في التاريخ أو بزيادة كلمات في مكان خال من المحرر ، وتهدف الإرادة إلى تزوير ذلك المحرر و إستخدامه.

أما التغيير بالحذف فيكون بحذف كلمة أو رقم أو أسم أو عبارة وردت في محرر ، أياً كانت الوسيلة التي استعملها المزور ، وسواء كانت بالكشط أو الشطب أو المحو بمادة كيميائية أو جزء

---

(1)عبد الباقي ، جميل ،(2001) ، الانترنت والقانون الجنائي ،الطبعة الأولى ، دار الفكر العربي ، القاهرة ، ص35.

(2)د. السعيد ، مصطفى السعيد ، (2000) ، قانون عقوبات القسم العام ، دار النهضة العربية ، القاهرة ، ص 100.

(3)د. رؤوف عبيد ، جرائم التزييف والتزوير،مرجع سابق ص139.

من المحرر بالحبر وخلافه ، على انه يلاحظ أن إعدام المحرر كله بإتلافه أو تمزيقه ايضاً يعتبر تزويراً كما نصت عليه المادة 662 في الفقرة الثالثة منه في قانون العقوبات الأردني على أنه يعتبر تزويراً في حالة إتلاف المحرر إتلافاً جزئياً أو كلياً.

وأما التغيير بطريقة التعديل فهو خليط بين طريقتي الحذف والإضافة كأن نستبدل كلمة بأخرى أو رقم برقم مثل تغيير تذكرة السفر بقطارات السكة الحديد[1].

والتغيير المعاقب عليه في هذه الحالة هو التغيير الذي تم على غير إرادة من حرر المستند أو المحرر ، فلو تم بناء على اتفاق بين الموقعين دون المساس بحق الغيير ، حصول اختلاف في مضمون المحرر نفسه ، إلا إذا تضمن ذلك مخالفة قواعد معينة نص عليها للقيام بتحرير المستند أو ما به من بيانات على نحو يخالف الحقيقة [2].

وعن إمكانية وقوع التزوير الإلكتروني بهذه الطريقة فهو أمر ممكن ذلك أن جهاز الحاسب الآلي حين يتلقى البيانات و المعلومات ضمن نطاقه الإلكتروني ، فانه يقوم بمعالجة هذه البيانات والمعلومات في ضوء طلبات وحاجات الجهة العامة أو الخاصة مستخدمة الحاسب الآلي ، إذ يتم معالجة النص بمعرفة الحاسب الآلي ، بناء على طلب ذوي الشأن ، ثم يظهر بعد ذلك مادياً في صورة مخرجات لهذا الحاسب ، وخلال مرحلة المعالجة يمكن التغيير في النص المعالج بالإضافة أو الحذف أو التعديل على النحو السابق بيانه ومن ثم يتحقق التزوير الإلكتروني بهذه الطريقة[3].

---

(1)مجموعة القواعد القانونية ،ج6،رقم253،ص659.

(2)د. فوزية ، عبد الستار ،شرح قانون العقوبات ، القسم الخاص ،مرجع سابق ،ص261.

(3)حسبو ، عمرو أحمد ، حماية الحريات في مواجهة نظم المعلومات، مرجع سابق ، ص 42.

3- **وضع أسماء أو صور أشخاص آخرين مزورة :**

ويتحقق التزوير المادي بهذه الطريقة حين يقوم الجاني بانتحال أو إبدال شخصيته بشخصية الغير، ويكون انتحال الشخصية حين يتسمى باسم شخصية آخر سواء كان هذا الشخص موجودا في حقيقة الواقع أو غير موجود ، وذلك بان يوقع على محرر بالاسم الذي انتحله أو يتقدم إلى المحكمة ويدعي انه المدعي ليقر بالتصالح مع المدعى عليه أو ترك الخصومة ، أو يتقدم بدلاً عن آخر ليؤدي الخدمة العسكرية عنه أو لتنفيذ عقوبة بدنية بدلاً عنه[(1)].

وقد يوقع المتهم بأسم من إنتحل شخصيته ، أو يمحوا الجاني أسمه ويوقع بدلاً عنه و إذا لم توجد هذه الآثار المادية كان التزوير معنويا ، كمن يحضر أمام الموظف العام ويدلي أمامه بأقوال ينسبها إلى ذلك الشخص في المحرر الذي قام بتدوينه[(2)] .

وقد لا حظ جانب من الفقه أن هذه الطريقة للتزوير المادي تثير تساؤلا حول المقصود منها؟

لأنها ليست طريقة مستقلة للتزوير، ذلك أن وضع اسم شخص آخر مزور لا يخرج عن كونه وضعا لإمضاء أو ختم شخص آخر، ولذلك يدخل ضمن الطرقة الأولى للتزوير المادي، وقد يكون مقصوداً بها وضع أسم شخص آخر في صلب المحرر أو تغيير لاسم وارد فيه باسم شخص آخر ، أو إضافة أسم للإمضاء، حيث تتوفر الطريقة الثانية من طرق التزوير المادي، إذن هذه الطريقة ليست مستقلة بذاتها [(3)].

---

(1)د. عوض محمد ،(1984) ، جرائم الأشخاص والأموال ،دار المطبوعات الجامعية ،الإسكندرية ، ص 200 .

(2)حسني ، محمود نجيب ، شرح قانون العقوبات ، القسم الخاص ، مرجع سابق ، ص236.

(3)د. فوزية ، عبد الستار ،شرح قانون العقوبات ، القسم الخاص ،مرجع سابق ، ص 263.

ومن ذلك أن قانون العقوبات المصري قام بتعديل المادة 211 و ألحق وضع الصور على المحررات بوضع الأسماء المزورة عليها ، وساوى بين الأمرين في التجريم والعقاب وبالتالي أصبح مفهوم المحرر متسعاً فلم يعد التزوير قاصرا على بيانات المحرر بل امتد إلى الصور الموضوعة عليه ، ويستوي أن يكون ذلك المحرر رسمياً أو عرفيا [1].

ويمكن تصور ذلك في المحررات الإلكترونية وحيث يمكن إعتبار الصورة أحد البيانات الجوهرية في المحررات الإلكتروني في التزوير الإلكتروني يمكن تزويرها عن طريق الحاسب الآلي، والأجهزة المساعدة لها ومنها الماسح الضوئي وذلك عن طريق إستنساخ الصورة ضوئيا ونقلها إلى الجهاز الحاسب الآلي وعرضها على الشاشة و يمكن استخراجها ورقياً عن طريق طابعة الحاسب الآلي أيضاً.

4- اصطناع المحرر او تقليده :

الاصطناع هو انشاء محرر لم يكن له وجود من قبل بأكمله ونسبته الى غير محرره[2] ، أو اصطناع شهادة ميلاد أو صك أو مخطوط ، وليس من الضروري وقوع التزوير بهذه الطريقة فقد يحاول الجاني تقليد خط من ينسب إليه المحرر وأن يوقع بإمضائه أو ختمه ، ومع ذلك فالغالب أن يكون الاصطناع مصحوبا بوضع أمضاء أو ختم مزور[3].

وهناك فرق بين التقليد والإصطناع ، ففي الإصطناع لا يهم الجاني مدى التشابه بين خطه وخط الغير، لأنه يضع محرراً جديداً بكامله ، بينما في التقليد فيتم انشاء المحرر على غرار اخر موجود يراعى فيه التشابه بينهما، ويتم التوقيع على المحرر المصطنع بتوقيع مزور لكي يستمد

---

(1)د. عوض محمد ، جرائم الأشخاص والأموال ، مرجع سابق ، ص178.

(2)قانون العقوبات العراقي رقم (111) لسنة 1969، المادة (291).

(3)رمضان، عمر السعيد ،(1965)،شرح قانون العقوبات ، القسم الخاص،الطبعة الأولى ،القاهرة ،دار النهضة العربية ، ص60.

المحرر قيمته القانونية من هذا التوقيع ، ولكن لايوجد تلازم بين التقليد والإصطناع فكلاهما مستقل عن الآخر[1].

والاصطناع الإلكتروني يتم من خلال إدخال المصطنع ما يريد من معلومات أو بيانات إلى الحاسب الآلي، ومن ثم ينسب صدورها إلى شخص ما أو جهة ما، ثم يستخرجها من الحاسب الآلي بوصفها منسوبة إلى ذلك الشخص أو تلك الجهة، ولذلك يعد تزييف العملة الورقية باستخدام الماسح الضوئي والحاسب الآلي من طرق الإصطناع كما هي من طرق التقليد ، لأن الاصطناع هو إيجاد محرر بأكمله ونسبه إلى غيره، ولا توجد صعوبة في إدخال عناصر المحرر المراد تزويره إلى الحاسب الآلي سواء عن طريق الماسح الضوئي، أو عن طريق لوحة المفاتيح، بل وعن طريق استدعاء المعلومات من الانترنت، ثم صياغتها في هيئة المحرر المزور الذي يطلبه الجاني ويطبعه ويستخدمه حسب رغبته[2].

أما فيما يخص **التقليد** ويقصد به المحاكاة و هو إنشاء محرر مماثل لمحرر أصلي، أو أن يحرر المتهم كتاباً بخط يشبه خط شخص آخر سعياً لأن ينسب اليه المحرر، وهو أيضاً صنع شئ كاذب يشبه شيئا صحيحا[3].

ويرى جانب من الفقه أن هذه الطريقة للتزوير لا تقع وحدها ، وإنما غالبا ما ترتبط بطريقة أخرى ، فلو قام الجاني بوضع إمضاء أو ختم مقلد على المحرر المقلد ، فقد توافر الى جانب طريقة التقليد طريقة أخرى من طرائق التزوير المادي ، ولكن البعض الآخر يرى أنه بالامكان أن

---

(1)حسني ، محمود نجيب ، شرح قانون العقوبات ، القسم الخاص ، مرجع سابق ، ص24.

(2)حجازي ، عبد الفتاح بيومي ، التزوير في جرائم الكمبيوتر والإنترنيت ،مرجع سابق ، ص226 وما بعدها.

(3)د. فوزية ، عبد الستار ،شرح قانون العقوبات ، القسم الخاص ،مرجع سابق ،ص 263.

يقع التزوير بطريقة التقليد لوحده دون ان يتداخل مع غيره من الطرائق ، وكان مثالهم على ذلك تقليد خط الغير في محرر موقع على بياض .

ونخلص مما تقدم الى إمكانية وقوع التزوير الإلكتروني بطريقة التقليد أياً كان المحرر أو المستند الذي يتم تقليده ولا يشترط أن يكون مكتوبا وإنما قد يتضمن صوراً أو رموزاً معينة لها دلالة خاصة يجري تقليدها على نحو متقن.

وأيضاً يعتبر التزوير الالكتروني هو أبسط وأسهل بكثير من التزوير في المحررات العادية لأنه لا يحتاج إلى إزالة باستخدام الأدوات والمواد الكيميائية لتغيير معاني الكلمات أو كشط توقيعات سابقة أو معاني، وإنما يحتاج فقط إلى إدخال كلمات أو تغيير معاني كلمات بالحذف أو الإضافة أو التعديل عليها عن طريق أدوات إلكترونية خاصة بل حاسوب أو غير ذلك ، وبذلك يصدر المحرر النهائي مطابقاً للأصل إن كان مزوراً في مضمونه.

ثانياً : طرق التزوير المعنوي وعلاقتها بالتزوير الإلكتروني :

إن طرق التزوير المعنوي يتكون من طريقتين حيث الطريقة الأولى هي تغيير إقرار أولي الشأن أما الطريقة الثانية هي جعل واقعة مزورة في صورة واقعة صحيحة ، أو جعل واقعة غير معترف بها في صورة واقعة معترف بها.

بينما يرى جانب من الفقه أن للتزوير المعنوي ثلاث طرق هي ذات الطريقتين السابقتين إلا انه فرق بين جعل الواقعة المزورة في صورة الواقعة الصحيحة وجعل الواقعة غير المعترف بها في صورة واقعة معترف بها وجعل كل منهما مستقل عن الاخر[1].

---

(1)حسني ، محمود نجيب ، شرح قانون العقوبات ، القسم الخاص ، مرجع سابق ، ص241.

وأياً كانت طرق التزوير المعنوي ، فهو تزوير يؤدي الى تغيير في مضمون المحرر أو ظروفه وملابساته لا في مادته أو شكله ، ولذلك فهو غالباً ما يقع عند إنشاء المحرر ، كما أنه لا يترك أثراً ظاهراً يمكن للحس إدراكه ، ولذلك فهناك صعوبة في إثباته وبذلك سنبين طرق التزوير المعنوي ونبحث في مدى إمكانية حصولها بالطرق الإلكترونية وكالآتي :

1- تغيير إقرار أولي الشأن الذي كان الغرض منه تحرير المحرر أو إدراجه فيه:

تفترض هذه الطريقة أن الجاني قد عهد اليه بتدوين المحرر وتسجيل بيانات فيه يمليها عليه صاحب الشأن ، مسجلا بدلاً عنها بيانات غير تلك التي اتجهت إليها إرادتهم ، ويقع التزوير بهذه الطريقة مادام صاحب الشأن لم يلاحظ التغيير قبل توقيعه على المحرر[1].

وهذه الطريقة للتزوير لاصعوبة في أن تتم بالطريق الإلكتروني، ذلك أن حسابات المؤسسات والشركات في الوقت الحالي غالبا ما تتم عن طريق الحاسب الآلي أو بوساطة برامج حسابية مخزنة على ذات الجهاز أو في أقراص مدمجة ، يمكن للجاني التلاعب في هذه البيانات معلوماتياً لمصلحته ، أما المحررات العادية فعندما يكلف المدين من قبل الدائن بأن يؤشر على ظهر سند الدين بما يفيد سداده جزء من الدين فيؤشر بسداد الدين كله أو معظمه على خلاف الحقيقة ، وهو تأشير ذو حجة لأنه تم بتوكيل من الدائن[2].

(1)د. فوزية ، عبد الستار ،شرح قانون العقوبات ، القسم الخاص ،مرجع سابق، ص282.

(2)نقض جنائي ، جلسة 18 / 5/ 1936م مجموعة القواعد القانونية ، ج3 ، رقم 473 ، ص603.

2- جعل واقعة مزورة في صورة واقعة صحيحة مع العلم بتزويرها .

وهي كل إثبات لواقعة على غير حقيقتها ، وعلى ذلك فكل تشويه أو تحريف يدخله كاتب المحرر على الوقائع التي يثبتها فيه عند تدوينه للمحرر يعد تزويرا معنويا بهذه الطريقة[1].

والتزوير في المحرر الرسمي بهذه الطريقة من الموظف المعهود إليه بتحريره كتقرير شيخ بلده في شهادة الشخص مطلوب للتجنيد أنه وحيد أبويه إثبات موظف على غير الحقيقة أن المستجوبين حضروا أمامه وتم سؤالهم ووقعوا[2].

كذلك فان بعض أجهزة التحقيق ومنها النيابة العامة في أمارة دبي بدولة الأمارات العربية المتحدة ، قد شرعت فيما يسمى (بالتحقيق الألكتروني) وهو أجتماع المحقق والمتهم في محبسه ، وكذلك الشهود ، ورجال الضبط في أماكنهم ، وذلك عن طريق دائرة تلفزيونية مغلقة عن طريق جهاز الحاسب الآلي ، ويدور التحقيق وكأنهم جميعا في حجرة وجها لوجه ، وهنا يمكن أن يقع التزوير في إثبات واقعة لم يتم الادلاء بها ، خاصة إعتراف المتهم ، أو عدم إثبات واقعة معينة، أو مكان حصول الواقعة أو زمانها وكل هذه الوقائع يمكن التلاعب بها، ويعد ذلك إنموذجا مثالياً في جعل واقعة مزورة في صورة واقعة صحيحة بالطريق الإلكتروني[3].

وأيضاً فيما يخص امكانية حدوث التزوير الإلكتروني بهذه الطريقة، فمن الممكن تصور ذلك عند قيام موظفي الحسابات ، من خلال أجهزة الحاسب الآلي بتحميل مكالمات تلفونية خاصة بشخص على شخص آخر ، أو إسقاطها عن شخص وتحميل ثمنها على آخر، وهذا يخص

---

(1)مجموعة القواعد القانونية ، ج3،ص603.

(2)د.عفيفي ، كامل عفيفي ، جرائم الكمبيوتر وحقوق الؤلف والمصنفات الفنية ودور الشرطة والقانون ، مرجع سابق ، ص255.

(3)مؤتمر عن الحكومة الالكترونية ، المركز التجاري بدبي للفترة من 21 – 22 / 1 / 2000م وتطرق المؤتمر الى التحقيق الجنائي الالكتروني ومشكلاته العملية .

المحررات الرسمية ، أما المحررات العادية فيمكن ذلك عندما يعطي طبيب شخصا ما شهادة مزورة تستوجب الاعفاء من الخدمة العسكرية في الدول التي تطبق نظام الخدمة الالزامية ، ومن ثم فالتزوير الإلكتروني فيه أمر وارد[1].

3- جعل واقعة غير معترف بها بصورة واقعة معترف بها :

يذهب جانب من الفقه الجزائي إلى أن هذه صورة من صور التزوير المعنوي ليست صورة مستقلة و إنما تدخل ضمن " جعل واقعة مزورة في صورة واقعة صحيحة " ومثالها أن يثبت مأمور الضبط واقعة اعتراف المتهم على حين انه لم يعترف ،أو أن يثبت الموثق أن البائع قد أقر بقبض الثمن على حين أنه لم يقر بذلك ، فالثابت في هذين المثالين أن الواقعة المزورة غير معترف بها وأن هذا التزوير جعلها واقعة معترف بها على حين أن المتهم لم يعترف ، كما أن البائع لم يقر بقبض الثمن[2].

ويقصد بهذه الطريقة أن يثبت كاتب المحرر إعتراف شخص بواقعة معينة في حين أنه لم يعترف بها في الحقيقة ، كما لو قام المحقق كذباً بتثبيت إعتراف المتهم بالتهمة المنسوبة اليه أو أن موثق العقد يثبت أن البائع أقر أمامه بقبض الثمن مع أنه لم يقر بذلك[3].

أما بالنسبة للتزوير الإلكتروني دائما متعلق بالتقدم العلمي والاعتماد على جهاز الحاسب الآلي وملحقاته في انجاز الأعمال لدى مؤسسات الدولة والقطاع الخاص ، فيمكن للموثق الذي يعتمد على جهاز الحاسب الآلي في إثبات البيانات التي يدلي بها الخصوم أن يغير من هذه الأقوال أو لا يثبتها أو يثبتها عكس ما تم بها الإدلاء بها على نحو يغير من مضمون المحرر

(1)رمضان، عمر السعيد ،شرح قانون العقوبات ، القسم الخاص ، مرجع سابق ، ص157.

(2)د. بنهام، رمسيس،الجرائم المضرة بالمصلحة العامة ، مرجع سابق ، ص190.

(3)رمضان، عمر السعيد ،شرح قانون العقوبات ، القسم الخاص ، مرجع سابق ، ص159.

الإلكتروني ، الأمر الذي يقوم به التزوير الإلكتروني ، ولذلك فالأمر مرجعه في الأعتماد أولاً وأخيراً على جهاز الحاسب الآلي وما يتبع ذلك من مخرجات قد تكون مزورة أو مطابقة حسب البيانات التي تتضمنها ومدى مطابقة هذه المخرجات للواقع(1).

وقد أخذ المشرع الأردني بكلا الطرق المادية والمعنوية ، حيث نصت المادة 262 من قانون العقوبات الأردني على أنه " – يعاقب بالأشغال الشاقة المؤقتة خمس سنوات على الأقل الموظف الذي يرتكب تزويرا ماديا في أثناء قيامه بالوظيفة ، إما باساءة استعمال إمضاء او ختم او بصمة أصبع او إجمالا بتوقيعه امضاء مزورا ، وإما بصنع صك او مخطوط وإما بما يرتكبه من حذف أو إضافة تغيير في مضمون صك او مخطوط.

حيث ذكر في هذه المادة الطرق المادية التي أخذ بها ، وكذلك أخذ بالطرق المعنوية في المادة 263 من قانون العقوبات الأردني حيث نصت على أنه " الموظف الذي ينظم سندا من اختصاصه فيحدث تشويشا في موضوعه او ظروفه إما باساءته استعمال إمضاء على بياض اؤتمن عليه، أو بتدوينه عقودا او أقوالا غير التي صدرت عن المتعاقدين او التي أملوها ، او باثباته وقائع كاذبة على انها صحيحة او وقائع غير معترف بها على انها معترف بها او بتحريفه أية واقعة أخرى بأغفاله أمرا او إيراده على وجه غير صحيح.

---

(1)عبد الفتاح بيومي حجازي ، التزوير المعلوماتي في جرائم الكمبيوتر والانترنت ، مرجع سابق ، ص245.

المطلب الثاني

الركن المعنوي لجريمة التزوير الإلكتروني

التزوير جريمة يتخذ ركنها المعنوي صورة القصد الجزائي في جريمة التزوير الإلكتروني و ينحصر مبدئياً في أمرين:

الأول : علم الجاني بأنه يرتكب الجريمة بجميع أركانها التي تتكون منها ، أي إدراكه أنه يغير الحقيقة في محرر بأحد الطرق المنصوص عليها قانوناً وأن من شأن هذا تغيير الحقيقة أن يترتب عليه ضرر مادي أو أدبي حال أو محتمل الوقوع يلحق بالأفراد أو الصالح العام(1).

ثانياً: اقتران هذا العلم باستعمال المحرر المزور فيما زور من أجله أي يتحقق هذا القصد بعلم الجاني أن من شأن فعله الذي يؤدي إلى التغيير الحقيقة في محرر بإحدى الصور أو الطرق التي نص عليها القانون و تؤدي أيظاً إلى حدوث ضرر للغير أو احتمال حدوثه مع انصراف إرادته إلى ذلك(2).

وجريمة التزوير الإلكتروني لا بد أن يتوافر في قصدها الجنائي العام العلم والإرادة ،أي أن تتوجه إرادة الجاني العمدية إلى ارتكاب الجريمة مع العلم بأركانها ، بالإضافة إلى قصد جنائي خاص ، حيث لا بد أن تتوافر لدى الجاني استعمال المحرر محل التزوير فيما زور من أجله ،

---

(1)د. رستم، هشام محمد فريد،قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق ، ص237.

(2)د.عفيفي ، كامل عفيفي ، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون ، مرجع سابق ص258.

وبه يتحقق القصد لقيام التزوير وانصراف إرادة الجاني إلى ارتكاب الفعل المادي المكون له مع علمه بذلك[1].

وكذلك يجب أن يعلم الجاني أنه يغير الحقيقة في محرر بإحدى الطرق التي نص عليها القانون وإذا كان لا يعلم ذلك انتفى القصد الجنائي لديه حتى لو كان جهله راجعاً إلى إهماله في التأكد من ذلك وهذا العلم مفترض فلا يدفع مسئوليته عن ذلك بجهله ، كما ينبغي أن يعلم الجاني أن فعله يسبب ضرراً فعلياً أو محتملاً للغير فإذا انتفى ذلك انتفى القصد ايضاً ، ولا يكفي توفر الأمرين السابقين بل يلزم بالإضافة إلى ذلك أن تتجه نية الجاني إلى استعمال المحرر فيما زور من أجله حتى ولو لم يستعمله ولا فائدة من نفي الجاني لهذه التهمة بدفع أنه لم يحصل على فائدة من جراء عمله [2].

إن عدم علم الجاني بركن من أركان الجريمة لا يترتب عليه تحقق القصد الجنائي لأنه يفترض بالفاعل أن يكون على علم بكل أركان جريمته وكذلك الحال إذا كانت الأفعال التي يقوم بها الجاني غير واضحة بصورة دقيقة ، فمن يقوم ببرمجة البيانات وتغيير الحقيقة في المحررات دون علمه بما سيحدثه هذا التغيير فإن القصد الجنائي ينتفي عنه وكذلك إذا أهمل ولم يتخذ الاحتياطات المطلوبة ، لأن الاهمال لا يحقق العلم في القصد الجرمي ، لكن الأضرار بالآخرين حتى لو كان محتمل الوقوع فإنه يحقق في جريمة التزوير الإلكتروني القصد الجنائي.

---

(1)فهد بن سعد بن عبد الله،(1996)،الأحكام الشرعية والنظامية لجرائم تزوير المحررات الرسمية ، رسالة لنيل شهادة الماجستير، ، المعهد العالي للعلوم الأمنية ، الرياض،، ص293

(2)د. رستم، هشام محمد فريد،قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق ، ص258.

المطلب الثالث

الركن الخاص لجريمة التزوير الإلكتروني

يعتبر عنصر الضرر من الأهمية بمكان في جرائم التزوير بشتى صوره ، إذ لا عقاب على التزوير إن لم يكن هناك ضرر يلحق بالغير ، ولا يفهم من ذلك ضرورة تحقق ضرر معين ، إذ يكتفي المشرع هنا باحتمالية وقوع الضرر ، لتحقق المسؤولية الجزائية ، ولا يختلف الأمر كثيراً في جرائم التزوير الإلكتروني ، فاشترط الضرر أمراً ثابتاً أيضاً .

ويقع الضرر بتمام التحريف المفتعل للحقيقة ، ثم استخدام تلك الصورة الجديدة للحقيقة ، سواء من قبل الفاعل أو حتى من قبل الغير ، الذي يعتمد في بناء قراره على هذه الحقيقة المفتعل بفعل الفاعل والتي يجهل زيفها ، والضرر في جريمة التزوير ، قد يكون حالاً أو محتمل الوقوع ، فردياً أو اجتماعياً ، مادياً أو أدبياً ، وسنتطرق إلى هذه الأنواع كالتالي[1] :

1- الضرر الفعلي والضرر المحتمل :

لم يعلق قانون العقوبات ، قيام جريمة التزوير على وقوع الضرر بالفعل بل يكفي أن يكون محتمل الوقوع ، يستوي في ذلك أن يكون احتمال وقوعه على المجني عليه الذي زور عليه المستند أو أي شخص آخر شرط أن يكون احتمال حصول ذلك الضرر امراً متوقعاً وفقاً للمجرى العادي للأمور لذلك فأن الوقت الذي يعول عليه في تقدير توافر احتمال الضرر هو وقت حصول التزوير.

(1)القاضي المناعسة،أسامة أحمد،والقاضي الزعبي،جلال محمد،جرائم تقنية نظم المعلومات الإلكترونية،مرجع سابق،ص166.

2- الضرر المادي والضرر الأدبي :

ويقصد بالضرر المادي ، ذلك الضرر الذي يصيب الذمة المالية للمضرور ، على نحو يؤدي لإنقاص عناصرها الإيجابية أي الحقوق ، وتحصيلها بالالتزامات السلبية ، وهذا النوع من الضرر هو الغالب لأنه يستهدف ثروة المجني عليه كتزوير عقد بيع ، أما الضرر الادبي يقصد به الضرر الذي ينال بالأذى شرف المضرور أو اعتباره أو عرضه أو كرامته فهو ضرر لا قيمة مادية له ، ويستوي في الضرر الذي تقوم به الجريمة التزوير أن يكون ذلك الضرر مادياً أو أدبياً[1].

يضاف لما تقدم أن الضرر إذا كان محتمل الوقوع وقت إرتكاب التزوير وكانت أركان التزوير الأخرى متوافرة في حينه ، كان التزوير قائماً وأن الجاني يستحق العقاب وإن حصل ما يحول دون تحقيق الضرر أو احتمال وقوعه ، فإذا ما اتهم شخص بتزوير سند دين بتغييره لتاريخ الاستحقاق ولكنه سدد الدين قبل تقديم القضية الى المحكمة وكان توجه القضاء بأن لا أهمية للتسديد بعد ارتكاب جريمة التزوير فعلا[2].

---

(1)د. فوزية ، عبد الستار ،شرح قانون العقوبات ، القسم الخاص ،مرجع سابق، ص276.

(2)ماهر عبد شويش الدرة ،(2002)، شرح قانون العقوبات – القسم الخاص – ، دار الفكر الجامعي ، القاهرة ، ص38.

الفصل الثالث

صور جريمة التزوير الإلكتروني

إن التزوير الإلكتروني يتخذ أشكالاً عديدة ، فقد يكون محرراً أو يكون عقدا، أو وثيقة هوية أو سفر، أو شهادة ميلاد أو وفاة أو بريد سواء كان عادياً أم إلكترونياً، كما قد يأخذ شكل بطاقة الكترونية مثل بطاقات التأمين الصحي، بطاقات التعريف ، البطاقات الإئتمانية وغيرها .

وهذه الوثائق تقترن بتوقيع الإكتروني الذي يثبت صحتها ، ونسبتها إلى صاحبها ، ولذلك فإن هذا التوقيع على قدر من الأهمية مما يقتضي حمايته جزائياً من الإعتداءات التي قد تقع عليه، ومن أخطر هذه الإعتداءات تزوير هذا التوقيع[1].

وسيعمل الباحث على تقسيم هذا الفصل إلى ثلاث صور وكل صورة من صور جريمة التزوير الإلكتروني سيتناوله الباحث في مبحث، حيث يتناول الباحث في المبحث الأول عن جريمة تزوير التوقيع الإلكتروني، و كذلك المبحث الثاني سيتناول فيه الباحث عن جريمة تزوير البطاقة الإئتمانية، أما في المبحث الثالث سيتناول فيه الباحث عن جريمة تزوير البريد الإلكتروني.

---

(1)حجازي ، عبد الفتاح بيومي ،(2007)،النظام القانوني للتوقيع الإلكتروني،الطبعة الأولى،دار الكتب القانونية،مصر،المحلى الكبرى،ص7.

المبحث الأول

جريمة تزوير التوقيع الإلكتروني

إن إنتشار الحاسب الآلي والإعتماد عليه في كافة مناحي الحياة بصورة شبه كلية ، فقد أفرز الواقع العملي طرق ووسائل حديثة في التعامل لا تتفق مع فكرة التوقيع بمفهومها التقليدي ، وعند إنتشار نظم المعالجة الإلكترونية للمعلومات التي بدأت تغزو الشركات والإدارات و البنوك إعتماداً على هذه الألات ، وأنه لا مجال للإجراءات اليدوية في ظلها ، فقد أصبح التوقيع اليدوي عقبة من المستحيل تكيفها مع النظم الحديثة للإدارة والمحاسبة ولهذا تم الإتجاه نحو بديل لذلك التوقيع اليدوي ، وهو التوقيع الإلكتروني[1].

لذلك جرمت بعض التشريعات فعل تزوير التوقيع الإلكتروني في نصوص خاصة، وذلك بعد أن أصبح له نفس القيمة القانونية التي يتمتع بها التوقيع العادي ، لذلك وضعت الحماية الازمة لتجنب مثل تلك الجرائم .

لذا سوف يتطرق الباحث عن تزوير التوقيع الإلكتروني في المطلب الأول عن مفهوم تزوير التوقيع ومن ثم نتطرق إلى الحماية الجزائية للتوقيع الإلكتروني وعلاقتها مع الجرائم الأخرى وذلك في المطلب الثاني.

---

(1)حجازي ، عبد الفتاح بيومي ،النظام القانوني للتوقيع الإلكتروني، مرجع سابق ، ص10.

المطلب الأول

مفهوم التوقيع الإلكتروني

إن ظهور الإنترنت وانتشار العولمة عمل على إلغاء كافة الحواجز بين الدول وصار استخدامه على وجه كبير لخدمة كافة المجالات الإقتصادية والثقافية والإجتماعية وتحقيق النفع والاستغلال التجاري ، وكان التوقيع في البداية تقليدياً يتم من خلال الكتابة إلا أنه نتيجة ظهور وسائل الإتصال الحديثة ظهرت الحاجة إلى استحداث صور جديدة للتوقيع تتناسب مع هذه المستحدثات.

وبعد ظهور المحررات الإلكترونية التي لابد لضمان صحتها وجود أمريين أساسيين هما الكتابة والتوقيع ، فالكتابة هي شرط بديهي لوجود المحرر ، أما التوقيع فهو السند الحقيقي لصحة المحرر وشرط أساسي لثبوت التصرف القانوني وحجية المحرر في الإثبات[1] ، لذلك قد يقع التزوير على التوقيع مثلما يقع على الكتابة في تغيير الحقيقة.

وقسم الباحث هذا المطلب إلى ثلاث فروع حيث تناول الباحث في الفرع الأول عن تعريف التوقيع الإلكتروني ، وتناول في الفرع الثاني عن صور التوقيع الإلكتروني ، وتناول أيضاً في الفرع الثالث عن حجية التوقيع الإلكتروني.

---

(1)عبد العال ، محمد حسين ، (1999)،ضوابط الإحتجاج بالمستندات العقدية في القضاء الفرنسي ،الطبعة الأولى ، دار النهضة العربية ، القاهرة ، ص 20 .

الفرع الأول : تعريف التوقيع الإلكتروني :

عرف بعض الفقهاء في القانون الجزائي التوقيع الإلكتروني بأنه حروف ، أو أرقام ، أو رموز، أو إشارات ، لها ، طابع منفرد ، تسمح بتحديد شخص صاحب التوقيع وتمييزه عن غيره ، ويتم اعتماده من الجهة المختصة[1].

وعرفه البعض الأخر بأنه : تعبيير شخص عن إرداته في الإلتزام بتصرف قانوني معين، عن طريق تكوينه لرموز سرية ، يعلمها هو وحده تسمح بتحديد هويته[2].

وكما عرفه القانون المصري في قانون التجارة الإلكترونية بأنها :" حروف أو أرقام أو رموز أو إشارات لها طابع منفرد تسمح بتحديد شخص صاحب التوقيع وتمييزه عن غيره"[3].

وأيضاً عرفه قانون إمارة دبي حيث جاء في قانون التجارة الإلكترونية الصادرة بإمارة دبي بأنه " توقيع مكون من حروف أو أرقام أو رموز أو صوت أو نظام معالجة ذيي شكل إلكتروني وملحق أو مرتبط برسالة إلكترونية ممهورة بنية توثيق أو إعتماد تلك الرسالة.

وعرفه أيضاً القانون الأردني في المادة (2) من قانون المعاملات الأردني في رقم 58 لسنة 2001 التوقيع الإلكتروني بأنه :"البيانات التي تتخذ هيئة حروف أو أرقام رموز أو إشارات أو غيرها وتكون مدرجة بشكل إلكتروني أو رقمي أو ضوئي أو أي وسيلة أخرى مماثلة في رسالة

---

(1)الجنبيهي ، منير محمد ، والجنبيهي ، ممدوح محمد ،(2004) ، التوقيع الإلكتروني وحجيته في الإثبات ، دار الفكر الجامعي، القاهرة،ص8.

(2)سليم ، أيمن سعيد ، (2004)،التوقيع الإلكتروني،الطبعة الأولى،دار النهضة العربية ، القاهرة ، ص22.

(3)حجازي ، عبد الفتاح بيومي ،النظام القانوني للتوقيع الإلكتروني ، مرجع سابق ، ص15 وما بعدها .

معلومات أو مضافة عليها أو مرتبطة بها ولها بعد يسمح بتحديد هوية الشخص الذي وقع عليها ويميزه عن غيره من أجل تبليغه وبغرض الموافقة على مضمونه [1].

وكما عرفه القانون العراقي في قانون التوقيع الإلكتروني والمعاملات الإلكترونية رقم 78 لسنة 2012 في المادة (1) بأنه :"علامة شخصية تتخذ شكل حروف أو أرقام أو رموز أو إشارات أو صوات أو غيرها وله طابع متفرد يدل على نسبته الى الواقع ويكون معتمداً من جهة التصديق[2].

وبعد ان تطرقنا لموقف التشريعات العربية المقارنه نجد ان اغلب التشريعات اتجهت الى اعطاء التوقيع الالكتروني حجيه في الاثبات وساوت بين التوقيع التقليدي والكتروني من هذه الناحية على الرغم من اختلاف الشروط التي تتطلبها اغلب هذه التشريعات الا ان الهدف واحد وكذلك نلاحظ اصرار هذه التشريعات على تضمين المحرر الالكتروني للتوقيع واعطائه الاهميه الازمه لما له من دور كبير في الاثبات.

الفرع الثاني : صور التوقيع الإلكتروني :

هناك عدة صور للتوقيع الإلكتروني وسيتطرق لها الباحث على مايلي :

1- نقل التوقيع العادي إلى توقيع إلكتروني بواسطة الماسح الضوئي :

يتم بواسطة الموقع نفسه الذي ينقل الوثيقة الموقعة يدويا إلى جهاز الماسح الضوئي فيقوم بقراءة وتصوير ونقل التوقيع العادي إلى داخل جهاز الكمبيوتر ، فيتحول إلى توقيع الكتروني

---

(1)العزام، سهيل محمد ،(2009)، التوقيع الإلكتروني،الطبعة الأولى ، المكتبة الوطنية ، عمان ، ص14 وما بعدها.

(2)قانون التوقيع الإلكتروني والمعاملات الإلكترونية العراقي ، برقم 78 ، لسنة 2012 ، المادة (1).

يمكن إضافته إلى الوثيقة المراد توقيعها، تظهر هذه الآلية بأنها سهلة إلا أنها غير آمنة على الإطلاق فيستطيع كل من يستعمل ذلك الجهاز بالاستيلاء عليه لذلك هذا النوع غير مستعمل بشكل واسع وغير معترف به كتوقيع قانوني[1].

2- التوقيع الكودي (باستخدام بطاقة ممغنطة والرقم السري):

هذه الصورة من أكثر الصور شيوعاً في حياتنا العملية حيث تقوم البنوك بإصدار بطاقات ائتمان وهنا يتمثل التوقيع الإلكتروني في إدخال البطاقة داخل الجهاز الآلي الخاص بالبنك بالإضافة إلى إدخال الرقم السري عن طريق الضغط على الأزرة الخاصة بجهاز السحب الآلي[2].

3- التوقيع باستخدام الخواص الذاتية (التوقيع البيومتري):

وهذا النوع من التوقيع يعتمد على خواص الكيميائية والطبيعية للأفراد وتشمل تلك الطرق ما يلي:

- البصمة الشخصية.
- مسح العين البشرية.
- التحقق من مستوى ونبرة الصوت.
- خواص اليد البشرية.
- التعرف على الوجه البشري.
- التوقيع الشخصي.

---

(1)جميعي ، حسن عبد الباسط ،(2000)،إثبات التصرفات القانونية التي يتم إبرامها عن طريق الإنترنيت ، دار النهضة العربية ، القاهرة ، ص35.

(2)الرومي ، محمد أمين، (2008)، النظام القانوني للتوقيع الإلكتروني،دار الكتب القانونية ، مصر ،ص48.

وهو ما يعني أنه يتم تعيين الخواص الذاتية للعين مثلاً عن طريق أخذ صورة دقيقة لها وتخزينها في الحاسب الآلي لمنع أي استخدام من أي شخص آخر بخلاف الشخص المخزنة الخواص الذاتية[1].

وهكذا الحال بالنسبة لبصمة الأصابع أو خواص اليد البشرية أو نبرة الصوت أو التوقيع الشخصي ففي كل حالة يتم أخذ صورة دقيقة و محددة وتخزينها في الحاسب الآلي بحيث لا يجوز لأي شخص عادي بالدخول لهذا الحاسب واستخدام ما به من معلومات وبيانات وخلافه إلا لهؤلاء الذين تم التحقق من مطابقتهم لما تم تخزينه على الحاسب الآلي سواء من بصمة الأصابع أو خواص اليد البشرية أو نبرة الصوت أو التوقيع الشخصي أو خواص العين أما إذا ثبت هناك إختلاف مهما كان بسيطاً فلا يتم السماح لهم بالدخول على الحاسب الآلي وتلك الطريقة تعد من أهم الطرق التي تحقق الأمان للحاسبات لأنها لا تسمح بالدخول لمن هم غير مسموح لهم بالدخول[2].

4- التوقيع الرقمي :

ينشأ هذا النوع باستخدام مفتاح خاص معتمد قانوناً من جهة مختصة بأصداره والتحقق من شخصية الموقع ، ويحتاج التوقيع الرقمي إلى وجود مراكز متخصصة تقوم بمراجعة محتويات الوثائق والتأكد من توقيع الاطراف باستخدام ملف PDF، ويقصد بالتوقيع الرقمي بيان أو معلومة

---

(1)الجنبيهي ، منير محمد ، والجنبيهي ، ممدوح محمد ، التوقيع الإلكتروني وحجيته في الإثبات ، مرجع سابق ، ص196.

(2)العزام، سهيل محمد ، التوقيع الإلكتروني ، مرجع سابق ، ص 21.

يتصل بمنظومة بيانات أخرى أو صياغة منظومة في صورة شفرة (كود) والذي يسمح لمرسل اليه إثبات مصدرها و الإستيثاق من سلامة مضمونها وتأمينها ضد أي تعديل أو تعريف[1] .

ويقوم هذا التوقيع على وسائل التشفير الرقمي الذي يعتمد على خوارزميات أو معادلات حسابية لضمان سرية المعلومات والإتصالات بطريقة آمنة عبر تحويله إلى معادلة لا يمكن لأحد يقراءتها إلا صاحب المفتاح الذي يملك الشفرة لفتحها،ثم يعمد مستقبل تلك الرسالة إلى فك التشفير بمفتاح آخر للحصول على المعلومات المرسلة ، فإذا ظهرت الرسالة بعد فك التشفير بصورة واضحة ومقروءة كان توقيع المرسل صحيحاً وهذا النوع من التوقيعات الإلكترونية يعتبر من أكثر التوقيعات الإلكترونية أمنه وآخر ما توصلت إليه التكنولوجي[2].

ويقوم هذا التوقيع على استعمال مفتاحين عام وخاص ، يتم استعمال المفتاح الخاص من صاحب التوقيع الالكتروني إما المفتاح العام فيمكن استعماله من الجميع للتأكد من موثوقية التوقيع والتأكد من هوية وشخصية الموقع وفقاً للقانون[3].

ويقصد بمفتاحين العام والخاص :

الأول : متاح شفرة عام : هو أداة إلكترونية متاحة للكافة تنشأ بواسطة عملية حسابية خاصة وتستخدم في التحقق من شخصية الموقع على المحرر والتأكد من صحة وسلامة محتوى المحرر الأصلي الإلكتروني .

---

(1)عبد الحميد، ثروت ،(2002)،التوقيع الإلكتروني ،الطبعة الثانية ، مكتبة الجلاء الجديدة بالمنصورة ، مصر ، ص61.

(2)عباس ، حفصي ، (2014) ، جرائم التزوير الإلكتروني ، أطروحة لنيل شهادة الدكتوراه ، جامعة وهران ، كلية العلوم الإنسانية والعلوم الإسلامية ، الجزائر ، ص92 .

(3)عباس ، حسن عبد الله ، التوقيع الإلكتروني ، (2003) ، التوقيع الإلكتروني، المجلد التاسع عشر ، مجلة العلوم الإقتصادية و الإدارية ، الكويت ، ص21.

الثاني : مفتاح شفرة خاصة : هو أداة إلكترونية خاصة بصحابها تنشأ بواسطة عملية حسابية خاصة وتستخدم في وضع التوقيع الإلكتروني على المحررات الإلكترونية ويتم الإحتفاظ بها على بطاقة ذكية مؤمنة ، وتستخدم هذه البطاقة وسيط إلكتروني مؤمن يستخدم في عملية إنشاء وتثبيت التوقيع الإلكتروني[1].

الفرع الثالث : حجية التوقيع الإلكتروني :

التوقيع في الشكل الكتابي يمكن أن يؤدي مجموعة متنوعة من الوظائف حسب طبيعة المستند الذي يحمل التوقيع ، فمثلاً التوقيع يمكن أن يكون دليلاً على نية الموقع الإقرار بتحريره نص المستند ، وأيضاً كدليل لأثبات في حالة قيام نزاع مستقبلي بين الأطراف ، وكذلك فهو أداة للتعبير عن إرادة الشخص في قبوله الإلتزام بمضمون العقد ووسيلة لتوثيق العقد وتأمينه من التعديل، كما أنه يميز شخصية صاحبه ويحدد هويته[2].

أما التوقيع الإلكتروني فخلاف قيامه بالوظائف السابقة فهو يتفوق على التوقيع التقليدي بالنظر إلى أن الإستيثاق من شخصية صاحب التوقيع يتم بشكل روتيني في كل مرة يتم فيها إستخدام الرقم السري أو المفتاح الخاص ، وبالتالي فإنه لا مجال للأنتظار حتى ينشب النزاع للبحث في مدى صحة التوقيع كما هو الشأن في معظم الأحوال بصدد المحررات الموقعة بخط اليد[3].

أضف إلى ذلك ما توفره التقنية الحديثة المستخدمة في تأمين التوقيع الإلكتروني عن طريق ما يسمى نظام المعاملات الإلكترونية الآمنة ، ويوفر هذا النظام التحقق من شخصية صاحب التوقيع.

(1)فهمي ، خالد مصطفى ، (2007)،النظام القانوني للتوقيع الإلكتروني في ضوء الإتفاقيات الدولية والتشريعات العربية ، الطبعة الأولى ، دار الجامعة الجديدة ، الإسكندرية ،ص62.

(2)إبراهيم ، خالد ممدوح ، (2009) ، التحكيم الإلكتروني في عقود التجارة الدولية ، طبعة الأولى ، دار الفكر الجامعي ، الإسكندرية ، ص405.

(3)جميعي ، حسن عبد الباسط ،إثبات التصرفات القانونية التي يتم إبرامها عن طريق الإنترنيت ، مرجع سابق ، ص46.

ورغم أن التوقيع الإلكتروني يمكنه القيام بذات وظيفة التوقيع التقليدي إلا أنه غير مستوف للشكل الذي يتطلبه القانون ، فهو نتاج حركة يد الموقع ، ولكنه لا يتم بشكل الحركة الذي حدده القانون المصري في الإمضاء أو الختم أو البصمة والذي لا يعتد بأي شكل آخر للتوقيع.

لذلك نجد التشريعات الحديثة والإتفاقيات الدولية أجازت أن يكون التوقيع اللازم بأي شكل أخر مثل الخاتم أو التثقيب أو الصورة المطابقة للأصل أو بوسائل إلكترونية ، فاتفاقية الأمم المتحدة للنقل البحري للبضائع 1978 (والمعروفة بقواعد هامبورج) نصت في المادة 3/14 على أنه " يجوز أن يكون التوقيع على سند الشحن بخط اليد أو طباعة أو بالصورة المطابقة للأصل أو بالتثقيب أو بالخاتم أو بالرموز أو بأية وسيلة آلية أو إلكترونية أخرى لا تخالف قانون البلد الذي يوقع فيه سند الشحن[1].

- ونصت المادة 1316 من القانون المدني الفرنسي الخاص بالإثبات والمواد المكررة لها على ما يلي : الدليل المقروء أو الدليل بالكتابة ينبع من حروف و أرقام أو من كل علامات أو رموز أخرى لها دلالة مفهومة أياً كان الوسيط الذي تكون عليه أو أياً كانت الصور إرساله أو بعثه .ومن خلال المواد 1/1316،3/1316 يتبين لنا أن التوقيع ضروري لاكتمال العمل القانوني ، وعنما يوضع من قبل الموظف عام فهو يضفي عليه مصداقية التصرف[2].
- وكذلك نصت المادة الرابعة عشر من قانون (التوقيع الإلكتروني وتكنولوجية المعلومات المصري) رقم 15 لسنة 2004 م ، منه أن :"للتوقيع الإلكتروني ، في نطاق المعاملات المدنية والتجارية و الإدارية ، ذات الحجية المقررة للتوقيعات في أحكام قانون الإثبات المصري

(1)إبراهيم ، خالد ممدوح ، التحكيم الإلكتروني في عقود التجارة الدولية ، مرجع سابق ، ص407.

(2)عباس ، حفصي ، جرائم التزوير الإلكتروني ، أطروحة لنيل شهادة الدكتوراه ، مرجع سابق ، ص94.

في المواد المدنية والتجارية ، إذا روعي في إنشائه و إتمامه الشروط المنصوص عليها في هذا القانون و الضوابط الفنية والتقنية التي تحددها الائحة التنفيذية لهذا القانون.

ونصت المادة الثامنة عشر من ذات القانون على أنه : "يتمتع التوقيع الإلكتروني و الكتابة الإلكترونية والمحررات الإلكترونية بالحجية في الإثبات إذا ما توفرت فيها الشروط التالية :

أ- ارتباط التوقيع الإلكتروني بالموقع دون غيره.

ب-وسيطرة الموقع وحده دون غيره على الوسيط الإلكترونية، مع إمكانية كشف أي تعديل أو تبديل في بيانات المحرر الإلكتروني أو التوقيع الإلكتروني[1].

وكل هذه الشروط منصوص عليها في نص المادة 6 من قانون الأونيسترال النموذجي.

- أما قانون التوقيع الإلكتروني والمعاملات الإلكترونية العراقي رقم 78 لسنة 2012 الذي يهدف في المادة (2) على ما يلي :

أ- توفير الإطار القانوني لاستعمال الوسائل الإلكترونية في اجراء المعاملات الإلكترونية.

ب-منح الحجية القانونية للمعاملات الإلكترونية والتوقيع الإلكتروني وتنظيم إحكامها.

ت-تعزيز الثقة في صحة المعاملات الإلكترونية ولامتها[2].

أما المادة الخامسة من نفس القانون التي نصت على ما يلي :"يحوز التوقيع الإلكتروني الحجية في الإثبات إذا كان معتمداً من جهة التصديق وتوافرت فيه الشروط الاتية :

---

(1)قانون التوقيع الإلكتروني وتكنولوجية المعلومات المصري ، رقم 15 لسنة 2004 ، المادة(14،18).

(2)قانون التوقيع الإلكتروني و المعاملات الإلكترونية العراقي ، رقم 78 ،لسنة 2012 ، المادة (2).

أ- أن يرتبط التوقيع الإلكتروني بالموقع وحده دون غيره.

ب-أن يكون الوسيط الإلكتروني تحت سيطرة الموقع وحده دون غيره.

ت-أن يكون أي تعديل أو تبديل في التوقيع الإلكتروني قابلاً للكشف.

ث-أن يكون ينشئ وفقاً للإجراءات التي تحددها الوزارة بتعليمات يصدرها الوزير[1].

- وكذلك القانون المعاملات الإلكترونية الأردني رقم 58 لسنة 2001 ، والذي جاء في جوهره مبني على القانون النموذجي للأونسيترال المتعلق بالتوقيعات الإلكترونية والمتعلق بالتجارة الإلكترونية . وقد استغل القانون النصوص المرنة في القانون النموذجي لإدراج بعض الأحكام والاستثناءات على القواعد العامة الواردة فيه.

- حيث نصت المادة (15)من القانون المعاملات الإلكترونية على أنه :"يعتبر التوقيع الإلكتروني محمياً إذا توفرت فيه الشروط التالية مجتمعة :

أ- إذا انفرد به صاحب التوقيع ليميزه عن غيره.

ب-إذا كان يحدد هوية صاحب التوقيع .

ت- إذا كان المتفاح الخاص خاضعاً لسيطرة صاحب التوقيع وقت إجراء التوقيع.

ث- إذا ارتبط بالسجل الإلكتروني بصورة لا تسمح بإجراء تعديل على ذلك السجل الإلكتروني بعد توقيعه دون إحداث تغيير على ذلك التوقيع[2].

وكذلك نصت المادة (16) من نفس القانون على أنه :" يعتبر الإلكتروني موثقاً إذا تحققت فيه جميع الشروط المذكورة في المادة 15 من هذا القانون وكان مرتبطاً بشهادة توثيق

---

(1)قانون التوقيع الإلكتروني والمعاملات الإلكترونية العراقي ، رقم (78) لسنة 2012 ، المادة (5).

(2)قانون المعاملات الإلكترونية الأردني ، رقم 15 لسنة 2015 ، المادة (15).

إلأكتروني صادرة وفقاً لأحكام هذا القانون والأنظمة و التعليمات الصادرة بمقتضاه ، وقت إنشاء التوقيع الإلكتروني عن إي من الجهات التالية :

أ- جهة توثيق إلكتروني مرخصة في المملكة .

ب- جهة توثيق إلكتروني معتمدة.

ت-أي جهة حكومية سواء كانت وزارة أو مؤسسة رسمية عامة أو مؤسسة عامة أو بلدية يوافق لها مجلس الوزراء على ذلك شريطة استيفاء متطلبات هيئة تنظيم قطاع الإتصالات .

ث-وزارة الإصالات وتكنولوجية المعلومات.

ج- البنك المركزي الأردني فيما يتعلق بالأعمال المصرفية أو المالية الإلكترونية[1].

ومن هنا نرى أن منهج الدول العربية يتشابه في رسم الشروط الواجب توافرها كي يكتسب التوقيع الالكتروني حجيته في الاثبات ، ومنها نستنتج الشروط العامة الواجب توافرها في التوقيع الالكتروني كي يتمتع بالحجية المرسومة للتوقيع العادي و هي على النحو الآتي :

أ- ان يكون التوقيع مرتبطا بالموقع وحده دون غيره .

وفي هذا الشرط يتوجبُ أن يكون التوقيع الالكتروني كالتوقيع التقليدي مميزا لصاحبه ، إذ أن التوقيع يعد علامة شخصية ومميزة لصاحبه ، إذ يستطيع وبطريقة واضحة ومحددة التعبير عن شخص صاحبه الذي وقعه وبتوافر هذا الشرط في التوقيع الالكتروني ، ويكون التوقيع شاهداً على نية الموقع من خلال تحريره العقد ، والاقرار بما ورد فيه وعلى نية الطرف الآخر الالتزام بمضمون العقد الموقع عليه ، وبهذا يتبين بوضوح إدراكه لامكانية ترتب نتائج قانونية على عملية التوقيع فيما يخص الموقع ، ولذا نجد أن التوقيع بحد ذاته من أهم صفاته أنه

---

(1)قانون المعاملات الإلكترونية الأردني ، رقم 15 لسنة 2015 ، المادة (16).

مميز لشخص صاحبه ومن ثم فإن لكل شخص توقيعاً ، فإذا كان التوقيع الالكتروني موثقا وفق ما تم الاتفاق عليه بين الاطراف ، فإنه يكون علامة مميزة لشخص الموقع ويرتبط به إرتباطا وثيقاً ، ومن ثم يشير الى شخص الموقع بطريقة لا لبس فيها ولا غموض(1).

ب-أن يكون الوسيط الالكتروني تحت سيطرة الموقع .

نستنتج من هذا الشرط أن يكون صاحب التوقيع منفرداً بتوقيعه إذ لا يستطيع أي شخص فك رموز هذا التوقيع الخاص به أو الدخول اليه بغير إذنه ، أي يجب أن تكون بيانات انشاء التوقيع تحت سيطرة الموقع وحده ، فكما بينا سابقاً أن التوقيع الالكتروني يتكون من حروف وأرقام لا يمكن لأحد أن يعرفها سواه ، ومن ثم عندما تتحول الحروف الى أرقام بوساطة رموز فك معينة ، فإن الموقع هو الوحيد القادر على استخدام هذه الرموز من أجل الوصول للتوقيع إذ أنه هو من ينشئ التوقيع الالكتروني بطريقته الخاصة به(2).

ج - أن يكون أي تعديل أو تبديل في التوقيع الالكتروني قابلا للكشف .

يتناول هذا الشرط مسالة مهمة هي ضرورة أن يكون هناك ارتباط بين التوقيع والمعلومات التي يجري التوقيع عليها ، فلا يمكن أن يكون التوقيع غير متعلق بمعلومات مرفقة معه ، لأنه لايمكن الوصول الى المحرر دون معرفة التوقيع الالكتروني إذا تم تغيير التوقيع الالكتروني نفسه، وبهذا فإننا نجد أن هذا الشرط يستلزم ضرورة تكامل البيانات المتعلقة بالتوقيع الالكتروني وترابطها ، بحيث يكون أي تغيير يلحق بالمحرر الالكتروني بعد توقيعه قابلا للكشف، ومن ثم إحداث أي تغيير أو تعديل على التوقيع الموضوع على المحرر الالكتروني يؤدي الى تعديل بيانات

---

(1)السوداني ، مثنى سعد جبار ، (2013) ، التزوير المعلوماتي في الحاسب الآلي ، رسالة لنيل شهادة الماجستير ، الجامعة المستنصرية ، بغداد ، ص116.

(2)عبيدات ، لورنس محمد ، (2005) ، اثبات المحرر الالكتروني ، الطبعة الأولى ، ، دار الثقافة للنشر والتوزيع ، عمان ، ص130.

المحرر كامله ، وهذا يجعل المحرر غير ذي حجة في الاثبات لأنه يؤدي الى زعزعة سلامة هذه البيانات والتوقيع الالكتروني.

د- التوثيق او التصديق .

كي يحصل التوقيع الالكتروني على الحجية اللازمة للاثبات ومن أجل الحرص على سلامة التعاقدات والمستندات الالكترونية ، فلا بد من التأكد من صحة التوقيع الالكتروني وسلامته ، فكما هو معلوم يتم توثيق التوقيع التقليدي بوساطة الشهود أو كاتب العدل ، أما التوقيع الالكتروني فيتم توثيقه من خلال هيئة أو إدارة مخولة للتثبت من التواقيع ومنح شهادة التصديق، وذلك للحد من جرائم الاحتيال أو التزوير التي يمكن أن ترتكب في حال كان التوقيع محرفا ، أو مزوراً مما يؤثر في مصداقية المعاملات الالكترونية[1].

ويلاحظ أن هذا الشرط قد اتفقت عليه معظم القوانين العربية والأجنبية لذلك نرى أن المشرع المصري قد أشار اليه في الفقرة (و) من المادة (1) من قانون تنظيم التوقيع الالكتروني رقم 15 لسنة 2004.

وكذلك نصت المادة (16) من قانون المعاملات الإلكترونية الأردني على التوثيق والجهات التي تصدر منه .

وأخير فإن القانون العراقي لم يخرج عن ذلك التوجيه عندما إشترط في الفقرة (اولا) من المادة (6) من قانون التوقيع الالكتروني والمعاملات الالكترونية أن تقوم الشركة العامة لخدمات

---

(1)عبيدات ، لورنس محمد ، اثبات المحرر الالكتروني ، مرجع سابق ، ص132.

الشبكة الدولية للمعلومات في وزارة الاتصالات منح تراخيص اصدار شهادات التصديق بعد استحصال موافقة الوزير وفقاً للقانون[1].

من ثم نجد أن المشرع العراقي قد حذا حذو المشرعين في اشتراط حصول التوقيع الالكتروني على شهادة التصديق من جهة المخولة باصدارها كي يكتسب حجية الاثبات .

المطلب الثاني

الحماية الجزائية للتوقيع الإلكتروني من التزوير

عند تطور تكنولوجيا المعلومات والاتصال الحديث في كل يوم أوضاع جديدة تحتاج الى تنظيم، ولا يتم ذلك إلا بقواعد قانونية جديدة تواجه هذا التطور السريع ، خصوصاً فيما يتعلق بالتوقيع الإلكتروني الذي يعتبر من أهم شروط الإثبات.

ويمكن تلمس هذه الحماية من خلال قانون الأونسترال النموذجي وهذا ما سيتناوله الباحث في الفرع الأول ، وكذلك بيان نصوص متفرقة في التشريعات المقارنة الذي تطرق اليها الباحث في الفرع الثاني ، وكذلك بيان خصائص التوقيع الإلكتروني في الفرع الثالث.

الفرع الأول : قانون الأونسترال النموذجي :

بين قانون الأونسترال النموذجي المتعلق بالتجارة الإلكترونية ، وكذلك التوقيع الإلكتروني القيمة القانونية لرسالة البيانات (للمحرر الإلكتروني) حيث ساوى بينها وبين المحرر العادي وذلك من خلال مجموعة كمن النصوص.

---

(1)قانون التوقيع الالكتروني والمعاملات الالكترونية العراقي ، رقم (78) ، لسنة 2012م ، المادة (6).

وإن المساواة بين رسالة البيانات (المحرر الإلكتروني) و المحرر الورقي من حيث القيمة القانونية مرهون بتوافر الشرائط اللازمة في التوقيع الإلكتروني حتى يؤدي وظيفته ، بل قد يؤدي ذات الدور الذي يؤديه التوقيع التقليدي ، ذلك أن التوقيع الأخير قد لا يجد له مكاناً في ظل تقدم نظم المعالجة الإلكترونية للبيانات والمعلومات[1].

ولذلك نظم قانون الأونسترال النموذجي للتوقيع الإلكتروني هذه المسائل حيث نص في المادة 6 على :

1- حيثما يشترط القانون وجود توقيع من شخص يعد ذلك الإشتراط مستوفى بالنسبة لرسالة البيانات (المحرر الإلكتروني) إذا إستخدم توقيع إلكتروني موثوق به بالقدر المناسب للغرض الذي أنشأت أو بلغت من أجله رسالة البيانات (المحرر الإلكتروني) في ضوء كل الظروف بما في ذلك أي إتفاق ذي صلة.

2- تنطبق الفقرة (1) سواء كان الإشتراط المشار فيها في شكل التزام أم كان القانون يكتفي بالنص على تبعات تترتب على عدم وجود توقيع.

3- يعتبر التوقيع الإلكتروني موثوقاً به لغرض الوفاء بالإشتراط المشار إليه في الفقرة (1) إذا:

أ- كانت بيانات إنشاء التوقيع مرتبطة في السياق الذي تستخدم فيه بالموقع دون أي شخص آخر.

ب- كانت بيانات إنشاء التوقيع خاضعة وقت التوقيع لسيطرة الموقع دون أي شخص آخر.

---

(1)حجازي ، عبد الفتاح بيومي ، (2004) ، التوقيع الإلكتروني في النظم القانونية المقارنة،الطبعة الأولى ، دار الفكر الجامعي ، الإسكندرية ، ص279.

جـ- كان أي تغيير في التوقيع الإلكتروني يجري بعد حدوث التوقيع قابلا للاكتشاف.

د- إذا كان الغرض من اشتراط التوقيع قانوناً هو تأكيد سلامة المعلومات التي يتعلق بها التوقيع ، وكان أي تغيير يجري في تلك المعلومات بعد وقت التوقيع قابلاً للإكتشاف[1].

لقد أعطت هذه المادة لرسالة البيانات (أي المحرر الإلكتروني) نفس القيمة القانونية للمحرر الورقي التي تقترن بتوقيع ، إذا اقترنت هذا المحررات بتوقيع الإلكتروني موثوق منه ، حيث يمكن نسبة المحررات لصاحبها ، ويتحقق ذلك إذ كانت بيانات إنشاء هذه التوقيع خاضعة عند التوقيع لسيطرة الموقع ، وكان بالإمكان اكتشاف أي تغيير يطرأ على المحرر بعد ربطها بهذا التوقيع.

وبذلك استكمل قانون الأونسترال النموذجي للتوقيع الإلكتروني مسألة القيمة القانونية لرسالة البيانات التي نظمها قانون اللأونسترال للتجارة الإلكترونية عندما أعطى لهذه الرسالة نفس القيمة القانونية التي للمحرر الإلكتروني كلما أمكن الإطلاع على البيانات الموجودة بها ، واسترجاعها عند الحاجة.

الفرع الثاني: الحماية الجزائية في التشريعات المقارنة :

نص المشرع المصري في قانون التوقيع الإلكتروني المصري رقم 15 لسنة 2004 للحماية القانونية للتوقيع الإلكتروني من خلال نصوص قانون التوقيع الإلكتروني ، حيث نص في

---

(1)قانون الأونسترال النوذجي للتحكيم التجاري الدولي ، لسنة 1985 ، المادة (6).

المادة 23/ب على معاقبة كل من: " أتلف أو عيب توقيعا أو وسيطا أو محررا الكترونيا أو زور شيئا من ذلك بطريق الإصطناع أو التعديل أو التحوير أو بأي طريق آخر[1].

يتضح من صيغة النص السابق أن المشرع المصري جمع عدة أنماط للسلوك الإجرامي الذي قد ينال التوقيع الإلكتروني إلى جانب التزوير في نص واحد ، مثل الإتلاف والتعييب ، وتعدد المحل الذي يقع عليه السلوك الإجرامي.

ويتمثل هذا السلوك الإجرامي في إتلاف أو تعييب المحرر أو الوسيط أو التوقيع الإلكتروني.

- وفعل الإتلاف يتحقق بإفقاد البرنامج الإلكتروني الخاص بالتوقيع الإلكتروني قدرته على العمل ، عن طريق نشر فيروس إلكتروني أو سكب ماء أو سائل على الوسيط الإلكتروني المحفوظ عليه ، ويكون تعيب التوقيع الإلكتروني كذلك بذات الوسيلة على النحو يفقده القدرة على العمل أو الصلاحية بصورة جزئية كأن يصدر التوقيع مشوهاً أو غير واضح.
- أما التعييب فأنه يتحقق بأي سلوك إجرامي يؤدي إلى إفقاد المحرر الإلكتروني وظيفة من وظائفه مثل طمس التوقيع الإلكتروني المدون عليه وطمس بعض الأسطر المكتوبة بطريقة إلكترونية فيه [2].
- وإلى جانب الإتلاف أو التعييب فقد عاقب المشرع كذلك على تزوير التوقيع الإلكتروني ويتحقق ذلك التزوير عن طريق الإصطناع أو التقليد لتزوير قائم بالفعل أو إنشاء منظومة توقيع إلكتروني ونسبتها إلى شخص من الأشخاص.

---

(1) قانون التوقيع الإلكتروني وتكنولوجية المعلومات المصري ، رقم 15 لسنة 2004 ، المادة(23).

(2) حجازي ، عبد الفتاح بيومي ،النظام القانوني للتوقيع الإلكتروني ، مرجع سابق ، ص542.

أما المشرع الإمارتي أيضاً حرص على تقرير حماية جنائية للتوقيع الإلكتروني في قانون المعاملات والتجارة الإلكترونية رقم 1 لسنة 2006 م، وأفرد الفصل التاسع منه للعقوبات على الجرائم الماسة بالتوقيع الإلكتروني.

وخطا أيضاً خطوة إيجابية في هذا الاتجاه بأن أصدر القانون الاتحادي رقم (5) لسنة2012 في شأن مكافحة جرائم تقنية المعلومات ، وتضمن القانون العديد من المواد التي من شأنها توفير الحماية القانونية لخصوصية ما يتم نشره وتداوله على الشبكة الإلكترونية زمن ضمنها التوقيع الإلكتروني.

حيث نصت المادة (11) من قانون الاتحادي لسنة 2012 بشأن تزوير التوقيع الإلكتروني على أنه " يعاقب بالحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين كل من استولى لنفسه أو لغيره بغير حق على مال منقول أو منفعة أو على سند أو توقيع هذا السند ، وذلك بالاستعانة بأي طريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة عن طريق الشبكة المعلوماتية أو نظام معلومات إلكتروني أو إحدى وسائل تقنية المعلومات[1].

وكذلك المشرع العراقي عمل على الحماية الجزائية للتوقيع الإلكتروني وذلك في مشروع قانون الجرائم المعلوماتية لسنة 2010 حيث نصت المادة (8) من مشروع قانون الجرائم المعلوماتي على أنه " يعاقب بالسجن المؤقت وبغرامة لا تقل عن (10000000) عشرة ملايين دينار و لا تزيد على (15000000) خمسة عشر مليون دينار كل من ارتكب أحد الأفعال الاتية :

---

(1)قانون الإتحادي الإماراتي ، رقم 5 ، لسنة 2012 ، المادة (11).

أ- زور أو قلد أو اصطنع بنفسه أو بواسطة غيره توقيعاً أو سنداً أو كتابة إلكترونية أو شهادة تصديق أو الترخيص بمزاولة خدمات التوقيع الإلكتروني وما في حكمها أو استعمالها عمداً بشكل غير مشروع[1].

وحسن فعل المشرع العراقي حيث لم يقتصر على التزوير فقط بل ذكر التقليد أيضاً لكي لا يترك مجال للشخص الذي استخدم التوقيع الإلكتروني ، ولابد من الإشارة هنا إلى أن المشرع العراقي لم يقتصر الجريمة على مجرد التزوير أو التقليد ، بل جرم فعل استعمال الغير مشروع وعاقبة بذات العقوبة المقررة لجريمة التزوير.

أما المشرع الأردني عمل على الحماية الجزائية للتوقيع الإلكتروني وجعله من ضمن البيانات أو المعلومات التي يتم التلاعب بها في قانون الجرائم الإلكترونية رقم 27 لسنة 2015 وحيث نصت المادة (4) منه على أنه : " يعاقب كل من ادخل أو نشر أو استخدم قصداً برنامجا عن طريق الشبكة المعلوماتية أو باستخدام نظام معلومات لإلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ أو التقاط أو تمكين الآخرين من الاطلاع على بيانات أو معلومات أو إعاقة أو تشويش أو إيقاف أو تعطيل عمل نظام معلومات أو الوصول اليه أو تغيير موقع الكتروني أو الغائه أو إتلافه أو تعديل محتوياته أو اشغاله أو انتحال صفته أو انتحال شخصية مالكه دون تصريح أو بما يجاوز أو يخالف التصريح بالحبس مدة لا تقل عن ثلاثة اشهر ولا تزيد على سنة وبغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) الف دينار[2].

---

(1)مشروع قانون الجرائم المعلوماتية العراقي لسنة 2010.

(2)قانون الجرائم الإلكترونية الأردني ، رقم 27 ، لسنة 2015 ، المادة (4).

لم ينص المشرع الأردني في هذا القانون صراحتاً على التوقيع الإلكتروني ولكن جعله من ضمن البيانات أو المعلومات التي يتم الأعتداء عليها بأي وسيلة من الوسائل التي نصت عليها المادة (4).

الفرع الثالث : خصائص جريمة تزوير التوقيع الإلكتروني :

تتميز جريمة تزوير التوقيع الإلكتروني بخصائص تجعلها مختلفة عن جريمة تزوير التوقيع العادي بحكم البيئة الإفتراضية التي تتم فيها، والوسائل التي ترتكب بها، مما يجعل هذه الجريمة تتميز بطبيعة مختلفة عن جريمة تزوير التوقيع العادي .

إن هذه الخصائص تتمثل في ارتباط جريمة تزوير التوقيع الإلكتروني بجريمة السرقة وجريمة الإختراق، وسنتطرق لها كما يلي :

اولا : ارتباط جريمة تزوير التوقيع الإلكتروني بجريمة السرقة وجريمة الإختراق :

إن التوقيع الإلكتروني هو منظومة مكونة من رموز وأرقام تميز صاحبها وتحدد هويته، ومن بين صور هذا التوقيع المعتمدة على فكرة الرموز نجد التوقيع الكودي أو السري الذي يرتبط غالبا بالبطاقات الممغنطة وغيرها من البطاقات الحديثة المشابهة والمزودة بذاكرة الكترونية ، ويتم تزويره بعد تعرضه للسرقة ، ثم استخدام الرقم والبطاقة في السحب[1].

أما صورة التوقيع البيومتري فتعتمد على الخواص الذاتية للشخص كقزحية العين، بصمة الأصبع ، نبرة الصوت وغيرها ، حيث يتم التقاط صورة دقيقة لعين المستخدم أو بصمة يده أو

---

(1) الجهني ، أمجد حمدان ، جرائم بطاقة الدفع الإلكتروني عبر شبكة الانترنيت ، http://www.cojss.com /replay.php?a=219.

صوته ثم تخزن بطريقة مشفرة في ذاكرة الحاسب الآلي والذي يقوم بمطابقة صفات المستخدم مع هذه الصفات المخزنة ولا يسمح له بالتعامل إلا في حال المطابقة ، لكن قد تتعرض هذه الصورة من التوقيع للإختراق بفك تشفير هذه البيانات ونسخها.

كما يمكن التقاط أرقام البطاقات عبر شبكة الإنترنيت بعد عملية اختراق واستخدامها باسم مالك البطاقة ، ففي عام 2004 أعلن مكتب التحقيقات الفيدرالي (FBI) أنه يحقق في حادث اختراق أجهزة كمبيوتر تم خلاله سرقة أرقام ثمانية ملايين بطاقة وفاء من شركة " processors international Data" ، وقد تستخدم تقنية تفجير الموقع التي تعتمد على ضخ مئات الآلاف من الرسائل الإلكترونية من جهاز القرصان إلى الجهاز المستهدف للتأثير على السعة التخزينية مما يشكل ضغطا يؤدي إلى تفجير الموقع وتشتيت البيانات المخزنة فيه، لتنتقل بعد ذلك إلى جهاز القرصان ، ليتجول في الموقع بسهولة ، ويحصل على كل ما يحتاجه من أرقام وبيانات خاصة ببطاقات الوفاء[1].

ثانيا : إستخدام أساليب تقنية في تزوير التوقيع الإلكتروني وصعوبة الكشف عنها :

لقد أصبح للتوقيع الإلكتروني دورا واسعا في مجال المعاملات والتوقيع على الوثائق نتيجة الثورة التكنولوجية والإعتماد على المعلوماتية في إنجاز هذه المعاملات، ومنها تلك التي تتم في القطاع الحكومي، حيث اتجه الواقع إلى البحث عن بديل للتوقيع التقليدي يستطيع أن يؤدي ذات الوظيفة من ناحية ويتكيف مع وسائل الإدارة الحديثة من ناحية أخرى، وهذا البديل يمكن أن يكون رقما سريا أو رمزا محددا وهو ما يسمى بالتوقيع الإلكتروني أي التوقيع الناتج عن اتباع إجراءات

---

(1)الجهني ، أمجد حمدان ، جرائم بطاقة الدفع الإلكتروني عبر شبكة الانترنيت ، مرجع سابق .

محددة تكنولوجيا تؤدي في النهاية إلى نتيجة معينة معروفة مقدما فيكون مجموع هذه الإجراءات هو البديل الحديث للتوقيع بمفهومه التقليدي وهو ما نسميه بالتوقيع الإجرائي(1).

إن هذا الإختلاف في طبيعة التوقيع يجعل تزويره مختلفا، ويصبح اكتشافه صعبا بالنظر لسهولة اكتشاف تزوير التوقيع الخطي بمضاهاة الخطوط ، فيما لا يترك تزوير التوقيع الإلكتروني أثرا ظاهرا باعتبار أن التوقيع الإلكتروني هو ختم الكتروني مشفر يملك مفاتحه صاحب التوقيع، ويتم تزويره باعتماد التوقيع نفسه عن طريق الحصول عليه ، وإن تزوير التوقيع الإلكتروني أمر صعب بالمقارنة مع تزوير التوقيع العادي، باعتبار أن التوقيع الإلكتروني عبارة عن منظومة رقمية مرتبطة بأنظمة أمان تقنية، حيث يعتمد التوقيع الرقمي – وهو أهم صور التوقيع الإلكتروني– على الدوال الرياضية واللوغاريتمات، كما أنه يعتمد على نظام المفاتيح العامة والخاصة، كما يؤمنه نظام التشفر.

إن التوقيع الإلكتروني يعد من قبيل البيانات الإلكترونية في صورها المختلفة التي تستخدم الرموز والحروف والتشفير، وهو غير الإمضاء الذي يعد كتابة يقوم بها الشخص تتخذ شكلا معينا مميزا يعتمده الشخص في التعبير عن إلتزامه بمحرر ما، كما أنه ليس من قبيل البصمة لأن هذا التوقيع يقوم على تقنيات لا تعد جزء من جسم الإنسان باستثناء التوقيع البيومتري(2).

ولذلك فإن تزوير التوقيع العادي يعتمد على تقليد الإمضاء أو الختم، مما يتطلب من الجاني معرفة فنية، بخلاف تزوير التوقيع الإلكتروني الذي يتطلب خبرة علمية في مجال الحاسوب والبرامج لأن طبيعة هذا التوقيع مختلفة تماما عن الأول.

---

(1)كردي ، أحمد السيد، توقيع الإلكتروني مفهومه التكنولوجي وحمايته ، 30 سبتمبر 2011،
(http://kenanaonline.com/users/ahmedkordy/posts/323677)

(2)حنان ، براهمي ،جريمة تزوير الوثيقة الرسمية الإدراية ذات الطبيعة المعلوماتية ، مرجع سابق ، ص257.

المبحث الثاني

جريمة تزوير البطاقة الإئتمانية

عند إندفاع العالم بقوة نحو المعلوماتية و البرمجيات الحديثة و التطور الإلكتروني أصبحت بطاقات الإئتمان هي وسيلة الدفع الأكثر إستخداماً وانتشاراً وقبولاً في العالم ، وذلك بعد أن نمت هذه البطاقات وتطورت تطوراً كبيراً حتى وصلت إلى ما هي عليه الآن.

وهكذا بدأت بطاقات الدفع الإلكتروني تحل محل النقود والشيكات ، وتستخدم على نطاق واسع ، نظراً لما تتمتع به من سهولة في الدفع ، وإمكانية التعامل بها محلياً وعالمياً ، فضلاً عن كونها ذات مسؤولية قانونية محدودة في حالة ما إذا تعرضت للفقد أو السرقة ، الأمر الذي دعا البعض إلى إعتبارها جزءاً لا يتجزأ من ثقافة النظام الاقتصادي العالمي المعاصر ، وقد صاحب انتشار بطاقة الإئتمان وتزايد حجم التعامل بهما نمو مطرد في الجرائم المصاحبة لاستخدامها ، فقد اعترف البعض في تزوير هذه البطاقات أو سرقتها واستخدامها بالتحايل في الاستيلاء على مال الغير ، ومما يزيد خطورة الأمر هو سهولة تزوير بطاقات الإئتمان من ناحية ، ولا توجد آلية عالمية لإحكام السيطرة على ضمان سرية بيانات هذه البطاقة من ناحية ثانية ، وصعوبة إثبات تزوير البطاقة والتلاعب فيها من ناحية ثالثة[1].

لكن قبل أن يتطرق الباحث في الحديث عن ذلك وغيره لابد من التكلم عن مفهوم البطاقة الإئتمانية و أنواعها وذلك ما يتناوله الباحث في المطلب الأول ، أما في المطلب الثاني سيتطرق الباحث عن الحماية الجزائية للبطاقة الإئتمانية من التزوير الإلكتروني.

---

(1)بصلة ، رياض فتح الله ، (1995) ، جرائم بطاقات الإئتمان ، الطبعة الأولى ، دار الشروق ، القاهرة ، ص79.

المطلب الأول

مفهوم البطاقة الإئتمانية

يقصد بالبطاقة الائتمانية ذلك النوع المحدد من البطاقات البلاستيكية الذي يعطي الحق لصاحبها بإجراء عمليات الشراء والسحب والائتمان ، وهي بهذا الوصف تتميز بعدة خصائص ما يستلزم بطبيعة الحال وجود نظام محكم كفيلاً بحمايتها.

نتيجة لما تقدم وجب أن نبين ذلك بتقسيم هذا المطلب إلى فرعين حيث نفرد الفرع الأول لتعريف البطاقة الائتمانية ونوضح في الفرع الثاني أنواع البطاقة الائتمانية.

الفرع الأول : تعريف البطاقة الائتمانية :

إن التعريف القانوني للبطاقة هو عقد بمقتضاه يقوم مصدر البطاقة بفتح حساب بمبلغ معين لمصلحة شخص هو حامل البطاقة يستطيع بواسطتها الوفاء بمشتريات لدى المحال التجارية ، وهذه الأخيره ترتبط مع مصدر البطاقة بعقد يتعهد بموجبه بقبولها الوفاء بمتطلبات حاملي البطاقة الصادرة من الطرف الأول ، على أن تتم التسوية النهائية بعد كل دورة محددة[(1)].

إما على مستوى فقهاء القانون وشراحه فهناك من عرفها على أنها بطاقة مصنوعة من مادة بلاستيكية تحتوي على شريط ممغنط يتضمن بيانات عن حساب العميل لدى البنك، كما يتضمن شريطاً لاصقاً مدوناً عليه توقيع صاحب الحساب بالإضافة إلى صورة شخصية للعميل، تستخدم هذه البطاقة في سحب المبالغ النقدية وفي دفع ثمن المشتريات.

---

(1)بصلة ، رياض فتح الله ، جرائم بطاقات الإئتمان ، مرجع سابق ، ص31.

وهناك من عرفها على أنها عبارة عن مستند يعطيه مصدره لشخص طبيعي أو اعتباري بناء على عقد بينهما يمكنه من شراء السلع والخدمات ممن يعتمد المستند دون دفع الثمن حالاً لتضمنه التزام المصدر بالدفع، كما يمكنه أيضاً من سحب النقود من البنوك[(1)].

وتكشف التعريفات عن العناصر الأساسية الواجب توافرها في البطاقة الإئتمانية ، وهي تتمثل في أطرافها الثلاثة :

1- الطرف الأول : الجهة التي لها حق إصدار البطاقة وقد تكون مؤسسة أو شركة أو بنكاً.
2- الطرف الثاني :"حامل البطاقة" ؛ وهو الشخص الذي يحصل على البطاقة الدفع الإلكتروني من جهة المصدرة ، بغرض استخدامه الشخصي لها باعتبارها وسيلة دفع لدى التجار للحصول على السلع والخدامات ، أو استخدامها في الحصول على احتياجاته النقدية من خلال أجهزة الصرف الأتوماتيكي في أنحاء العالم كافة.
3- الطرف الثالث :"القابل" ويسمى في العرف المصرفي والتجاري بالتاجر؛ وهو الجهة التي تقبل الوفاء بواسطة بطاقات الدفع الإلكتروني نظير ما يقدمه لحامليها الشرعيين من سلع أو خدمات ، وذلك في مقابل توقيعهم له على إشعارات البيع[(2)].

وعند التطرق إلى هذا الموضوع يعرف الباحث أن البطاقة الإئتمانية هو عقد بين مصدر البطاقة الذي عمل على فتح إعتماد بمبلغ معين لمصلحة الطرف الآخر هو صاحب أو حامل البطاقة الذي يستطيع بواسطتها دفع أو الوفاء بمشترياته لدى محلات التجارية التي ترتبط من جهة آخرى مع مصدر البطاقة بعقد الذي يتضمن بقبول الوفاء من صاحب أو حامل البطاقة الإئتمانية.

---

(1)د. زين محمد الزماني، (1421 هـ) ، التزوير والتزييف عن طريق بطاقات الائتمان، مجلة المحامي، ع3، الرياض ، ص52.

(2)الصغير ، جميل عبد الباقي ،(1999)، الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة ،الطبعة الأولى ، دار النهضة العربية ، القاهرة ، ص11 وما بعدها.

الفرع الثاني : أنواع البطاقات الائتمانية :

تتعدد أنواع البطاقات الائتمانية على مستوى العالم فتوجد مؤسسات مالية عالمية تتنافس في الامتيازات التي تقدمها، ما أدى لنشوء العديد منها على الرغم من احتفاظها بالفكرة الأساسية التي بنيت عليها ، ولذلك نبين تلك الأنواع على ما يلي :

اولاً : أنواع البطاقات الائتمانية بناء على الجهة المصدرة :

يشترط كأصل عام أن تصدر البطاقة الائتمانية من قبل شخص معنوي يمارس النشاط التجاري المنصب على إصدار البطاقات وفق ترخيص معين وهذه الشروط حين توفرها تسمح الحق للمؤسسة المصرفية بإصدار البطاقة بشكل عام دون تحديدها بنوع معين ومن هنا اختلفت الطرق التي تصدر بها البطاقة الائتمانية بين المؤسسات وكانت على عدة طرق ، فالنوع الأول يكون ذا طابع محلي يصدر باتفاق المؤسسات العالمية والمصارف على مستوى الدول بإعطاء تفويض يسمح لها إصدار البطاقة الائتمانية بشرط احتواء كل منها اسم المنظمة وشعارها مع الشعار الموحد الذي يمثل التكتل بين تلك المؤسسات(1).

أما النوع الثاني يكون ذا طابع دولي فتصدر البطاقة عن طريق رعاية مؤسسة دولية واحدة تشرف على الفروع المنتشرة في العالم بحيث تحتكر وحدها إصدار هذه البطاقة كما هو الحال في (أميركيان اكسبريس وغيرها...) وتكون عادة غير محدودة الاستخدام ، وقد تكون محدودة حين تصدر عن طريق مؤسسات تجارية.

---

(1)الصغير ، جميل عبد الباقي ، الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة ، مرجع سابق ، ص37.

ويوجد كذلك بطاقات ائتمانية محدودة تستخدم عن طريق الانترنت في نطاق العالم الافتراضي فقط وتصدر من قبل مؤسسات مصرفية تتعامل بنظام التحويل الالكتروني لغرض شراء الاحتياجات عن طريق التعامل مع الزبون من مكان تواجده بشكل مباشر الا انها تبقى محتفظة بالفكرة الاساسية التي بنيت عليها البطاقة الائتمانية على الرغم من اقتصارها غلى شبكة الانترنت في التعامل[1].

ثانياً : أنواع البطاقة الائتمانية بناء على الحدود الائتمانية :

نظراً للوظيفة الائتمانية التي تتميز بها البطاقة الائتمانية نجد أن الشركات الراعية ألزمت مصدري البطاقات ان يعينوا حد أقصى لكل عملية منفذة بواسطة البطاقة وباختلاف نشاط المؤسسة كما هو الحال في الفنادق والمطاعم والوكالات السياحية وذلك بسبب ان قيمة الفاتورة حين يكون مقيد بعد تمريرها في الة السحب او الدفع توفر القيمة المطلوبة دون الحاجة للاتصال المباشر لمعرفة الرصيد المتوفر بالبطاقة بالاعتماد على الحد الائتماني لها.

ولذلك هناك ائتمان لكل نوع من أنواعها يتناسب مع قدرته المستخدم الائتمانية ، فمثلا نجد أن بطاقة الفيزا كارت تكون أما فضية والتي تكون ذات ائتمان محدود والتي تمنح لأغلب العملاء عند انطباق المتطلبات الضرورية فيهم ويكون لحاملها القدرة بواسطة هذه البطاقة على شراء السلع والخدمات من التجار والسحب النقدي من البنوك والصراف الآلي، أو قد تكون بطاقة ذهبية تمنح للعملاء أصحاب الضمان مالي الجيد مع إعطائه امتيازات أخرى كتأمين على الحياة والحجز في مكاتب السفريات والفنادق والتأمين الرسمي[2].

---

(1)سفر ، احمد (2008)، انظمة الدفع الالكتروني، الطبعة الأولى ، منشورات الحلبي الحقوقية ، بيروت ، ص96.

(2)مجلة المحقق الحلي للعلوم القانونية والسياسية ، العدد الثاني ، مرجع سابق ، ص117.

ولذلك تتعدد الضمانات بحسب كل نوع من أنواع البطاقة الإئتمانية وحدودها الائتمانية ، فقد يشترط توافر ضمان شخصي عندما تكون البطاقة الممنوحة ذات سقف ائتماني عالي من قبل احد رجال الإعمال المعروفين أو الشخصيات العامة ، وقد تتطلب أحيانا ضمان عيني جزئي يحفظ في تلك المؤسسة بشرط أن يكون اقل من الحد الأقصى وهذا النوع يمنح للأشخاص الذين لا تتوفر فيهم الثقة الكافية[1].

ثالثاً : أنواع البطاقات الائتمانية بناء على وظيفتها :

تتعدد البطاقات الإئتمانية بالنظر إلى وظيفتها فتكون تارة بطاقة اقتراض مهمتها الأساسية الوفاء والدفع الالكتروني تخول صاحبها الحصول على السلع والخدمات مقابل الدفع الفوري في حال وجود رصيد والاقتراض بواسطة البطاقة الائتمانية في حال عدم وجود رصيد على أن يتم التسديد خلال الفترة المسموح بها وفي حال تأخره عن التسديد يتم تحميل المبلغ الأصلي فوائد مالية عن طريق كشف مالي يرسل إلى العميل بحسب البيانات المالية الموجودة لدى المؤسسة المصدرة للبطاقة، أو قد تكون عبارة عن بطاقة خصم شهري والتي تمثل الصورة الأولى التي ظهرت بها البطاقة في العام 1951 لغرض تسهيل الحركة التجارية في المطاعم والمتاجر ، وثم صدرت بعد ذلك ما يطلق عليها كروت التسلية أو المتعة وتكون فترة ائتمانها لمدة شهر ويلتزم حامل البطاقة التسديد نهاية الشهر أو التعرض للمسائلة القانونية[2].

أو قد تكون عبارة عن بطاقات الخصم الفوري وهي من أكثر البطاقات المنتشرة في أوربا وهذا النوع من البطاقات يستخدم كأداة للوفاء وتعتمد بالدرجة الأساس على وجود رصيد متوفر ليتم

---

(1)حسن ،إيهاب فوزي ، (2006) ،الحماية الجنائية والأمنية لبطاقات الائتمان ، أطروحة دكتوراه مقدمة إلى أكاديمية الشرطة في مصر ، ص20.

(2)حسن ، إيهاب فوزي ، الحماية الجنائية والأمنية لبطاقات الائتمان ، مرجع سابق ، ص23.

الاستقطاع المباشر عند التعامل أما في حالة تجاوزه الحد المسموح فيجب أن يتم اخذ موافقة قسم الائتمان بالمصرف المصدر ثم أذا حصلت الموافقة يحسب المبلغ الإضافي على نظام البطاقة الائتمانية[1].

وتكون في بعض الأحيان بطاقة صراف الآلي والتي يقتصر دور هذه البطاقة على وجود مبالغ مالية مودعة بالمصرف مسبقا وله حق السحب خلال اليوم الواحد بحد معين بحيث لا يمكنه أن يتجاوزه ويتم التعامل بهذا النوع بواسطة أجهزة الكترونية مساعدة ، وكذلك توجد البطاقة الائتمانية على شكل بطاقة انترنت وهي مصدرة خصيصا للتسوق الالكتروني و لتجنب حالات الاحتيال وتمنح صاحبها حماية أمنية من المخترقين مع سرية كبيرة تمنع من سرقة أرقام البطاقات[2].

المطلب الثاني

الحماية الجزائية للبطاقة الائتمانية من التزوير

تتحدد الحماية الجزائية لجريمة تزوير البطاقة الائتمانية وفق مجموعة من النصوص الواردة في الاتفاقيات الدولية والتشريعات الداخلية، لتضفي حماية من الاعتداءات الواقعة عليها والمتمثلة بالأفعال المحققة لتغيير الحقيقة .

وللحديث بشكل مفصل عن هذا المطلب نفرد في الفرع الأول الحماية الجزائية للبطاقة الائتمانية على المستوى الدولي، ثم نفرد في الفرع الثاني الحماية الجزائية في التشريعات المقارنة.

---

(1)مرهج ، محمد حماد ، (2009) ، الحماية الجنائية لبطاقات الائتمان الممغنطة ، دار الكتب القانونية ،مصر ، ص44 .

(2)عبد الحكيم ، سامح محمد ، (2003) ، الحماية الجنائية لبطاقات الائتمان ، دار النهضة العربية ، القاهرة ، ص 76.

الفرع الأول : الحماية الجزائية على مستوى الدولي :

هناك عدة إتفاقيات نصت على حماية البطاقة الإئتمانية على مستوى الدولي من أجل مكافحة مثل تلك الجرائم ، ومن أهم هذا الإتفاقيات هي إتفاقية الدولية المعقودة برعاية منظمة الشرطة الدولية ، وكذلك اتفاقية بودابست ، وسنتحدث عنهم بشكل مفصل في النقاط التالية :

اولاً : الاتفاقيات الدولية المعقودة برعاية منظمة الشرطة الدولية :

لمنظمة الشرطة الدولية (الانتربول) دور هام وفعال في متابعة الظواهر الإجرامية بصورة عامة والإجرام الإلكتروني على وجه الخصوص ، من خلال الأقسام والشعب التي تتكون منها المنظمة كشعبة الإجرام الاقتصادي والمالي ، وشعبة التقصي الآلي وتحليل المعلومات ، وغيرها من الأقسام الخاصة المهتمة بمتابعة الظواهر الإجرامية على المستوى الدولي ، وهي كذلك تقوم بالتعاون المتبادل في مجال المعلومات ومكافحة ومنع انتشار الجرائم من خلال الخطط التي تضعها والمتابعة المستمرة للإجرام الدولي[(1)].

وبخصوص دورها في متابعة الجرائم الواقعة على البطاقة الائتمانية فقد نظمت السكرتارية العامة أولى مؤتمراتها الدولية بخصوص الاحتيال والغش في البطاقة الائتمانية في عام 1994 ونلخص عن هذا المؤتمر توصيتين هما:

1- على الدول الأعضاء مراجعة تشريعاتها وقوانينها الخاصة ببطاقات الائتمان بما يتضمن تجريم كل فعل يتضمن تصنيع و امتلاك أي معلومات غير قانونية تم الحصول عليها بطريق غير مشروع أو استخدامها في نظام بطاقات الائتمان.

---

(1)صوالحة، معادي اسعد ، (2011) ، بطاقات الائتمان النظام القانوني واليات الحماية الجنائية و الأمنية – دراسة مقارنة ، المؤسسة الحديثة ، لبنان ،ص489.

2- إنشاء مجموعات عمل بوليسية من خبراء متابعة جرائم الغش والاحتيال على المستوى الدولي التابعين لبوليس (هونك كونك والشرطة الكندية والخدمة السرية الأمريكية وخدمة الاستخبارات القومية الجنائية النيوزلندية ومندوبين من منظمات الائتمان) لمكافحة هذا النوع من الأجرام ووضع الأسس الخاصة لتبادل المعلومات و الحد منه[1].

وبناء على هذه التوصيات عقدت خمس اتفاقيات بين المنظمات المصدرة للبطاقات الائتمانية وأجهزة المنظمة لتوثيق التعاون ولمكافحة الجرائم الواقعة على البطاقة الائتمانية.

ثانياً : أتفاقية بودابست :

سميت الاتفاقية كذلك باتفاقية مكافحة الإجرام السيبيري أو الإجرام الافتراضي أو الكوني وتم توقيعها في عام 2001 ، تضمنت المذكرة الإيضاحية للاتفاقية (ظهور الثورة الالكترونية في عالم المعلومات ضاعف من ارتكاب الجرائم الاقتصادية ومنها الغش والاحتيال والتزوير في بطاقات الائتمان فالأصول المالية التي يتم تداولها بواسطة الحاسب الآلي أصبحت هدفا للتداول)[2].

وتتضمن هذه الاتفاقية عدة مواد تناولت أوجه الإجرام الإلكتروني ، فقد عرفت المادة (7) التزوير بأنه (إدخال أو أفساد أو تعطيل أو محو أو شطب عن قصد وبدون وجه حق) والتزوير وفقا لهذا المفهوم يعني أن الصور التي يتحقق بها التزوير الإلكتروني هي الإدخال أو التعطيل أو الإفساد أو المحو أو الشطب آذ ارتكبت عن قصد وبدون وجه حق في المعطيات الالكترونية ،

(1)الكعبي ، محمد عبيد ، (2009) ، الحماية الجنائية للتجارة الالكترونية ، أطروحة لنيل شهادة الدكتوراه ، كلية الحقوق ، جامعة القاهرة ، ص 276.

(2)احمد ، هلالي عبد الإله ، (2003) ، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، ص60.

والحصول على معطيات غير صحيحة بهدف استعمالها بطريق غير مشروع كما لو كانت تلك الوسائط صحيحة و أصلية ، أما المادة (8) نصت على (يجب على كل طرف أن يتخذ الإجراءات التشريعية أو أي إجراءات أخرى يرى أنها ضرورية للتجريم تبعا للقانون الوطني ، وتجريم أي فعل يتسبب في إحداث ضرر مالي للغير عمدا وبدون وجه حق عن طريق ما يلي :

1- الإدخال أو الإتلاف أو المرور ضمن نشاطات الحاسب الآلي.

2- كل شكل من إشكال الاعتداء على الحاسب الآلي بنية الغش أو أي نية إجرامية مشابهه للغش من اجل الحصول بدون حق على منفعة اقتصادية لمرتكب الفعل) [1].

ويتضح من النص أعلاه أن التزوير الواقع على البطاقة الائتمانية وفقاً لما جاءت به الاتفاقية قد نص عليه في المادة (7) التي نظمت الأفعال التي يقع بها التزوير ، ألا أن ما تجدر الإشارة إليه هنا هو عدم تطرق هذه المادة للتزوير الواقع بطريق التغيير واكتفى النص بالإدخال أو المحو ،أما المادة (8) فقد أوجبت على الدول اتخاذ الإجراءات التشريعية اللازمة لتجريم هذه الأفعال لضمان مسالة المزورين وفقاً للقوانين الداخلية وهي انتقاله نوعية تؤكد الاتجاه الدولي لوضع نصوص قانونية تعالج الجريمة المعلوماتية، وعلى ذلك فهي تشكل أساس قانوني كفيل لحماية البطاقة ولأجهزة الصراف الآلي من التلاعب ويحمي كذلك أجهزة جمع النقاط المثبتة لدى التجار المخصصة لإتمام المعاملات وغيرها من الأجهزة الإلية التي تعتمد في طريقة عملها على الحاسب الآلي.

---

(1)مجلة المحقق الحلي للعلوم القانونية والسياسية ، العدد الثاني ، مرجع سابق ، ص129.

ويلاحظ كذلك أن هذه الاتفاقية قد تطرقت لجانب مهم في مجال الحماية الجنائية للبطاقة الائتمانية من خلال إيرادها لمجموعة من الإجراءات في المواد (14-15) الخاصة بالضبط والتفتيش[1].

الفرع الثاني : الحماية الجزائية في التشريعات المقارنة :

نظراً لخطورة التلاعب في بطاقات الدفع الإلكتروني ، أياً كانت صورتها ، فأنه يجب مواجهة هذا التلاعب ، للحد منه وتجنيب المجتمع المخاطر المالية والإقتصادية التي تترتب عليه، ولذلك من وضع تشريعات تعمل على ردع مثل تلك الجرائم وسوف نتطرق إلى مجموعة من التشريعات المقارنة في شأن البطاقة الائتمانية.

- وصدر التشريع الفرنسي في قانون العقوبات سنة 1994/12/16ونظم التزوير بشكل جديد فنصت المادة (1/441) على أن التزوير هو (كل تغيير تدليسي للحقيقة يكون من طبيعته أن يسبب ضرر بأي وسيلة مهما كانت في محرر أو أي سند للتعبير عن الرأي والذي من ممكن أن يكون له الأثر في أنشاء دليل على حق أو فعل تكون له نتائج قانونية ، وقد اتجه الفقه الفرنسي لاعتبار البطاقة مستند معد أو قادر على أقامة الدليل على حق أو واقعة تحدث نتائج أو أثار قانونية [2].
- وأما التشريع العراقي لم ينظم في قانون العقوبات العراقي جريمة تزوير البطاقة الائتمانية ، فقد جاءت نصوصه خالية من الإشارة إلى التزوير الواقع عليها ، لذلك يتم الرجوع إلى قانون العقوبات في نصوصه التقليدية ، فقد نظمت جريمة تزوير المحررات الرسمية

---

(1)محمود ، لمى عامر ، (2008) ، الحماية الجنائية لوسائل الاتصال – دراسة مقارنة ، اطروحه لنيل شهادة الدكتوراه ، كلية القانون ، جامعة بابل ، العراق ، ص42.

(2)زين الدين ، بلال أمين ، جرائم نظم المعالجة الآلية للبيانات ، مرجع سابق ، ص331.

والعرفية في الفصل الثالث من الباب الخامس تحت عنوان الجرائم المخلة بالثقة العامة في المواد (286- 298) ، حيث عرفت المادة (286) التزوير بأنه (كل تغيير للحقيقة بقصد الغش في سند أو وثيقة أو أي محرر أخر بإحدى الطرق المادية و المعنوية التي نص عليها القانون ، تغيير من شانه إحداث ضرر بالمصلحة العامة أو مصلحة احد الأشخاص)[1].

إلا أن هناك مشروع قانون (الاتصالات والمعلوماتية) لمكافحة تلك الجرائم وخصوصاً جريمة تزوير البطاقة الائتمانية.

ويعد مشروع قانون الاتصالات والمعلوماتية من المشاريع المستقبلية التي تهدف لعلاج الحالات غير المنصوص عليها من الجرائم الإلكترونية ولغرض سد النقص التشريعي مع تعزيز الحماية القانونية اللازمة .

وكما ضم المشروع الجرائم المعلوماتية عدداً من المواد التي تناولت الجرائم الإلكترونية ومنها جريمة تزوير البطاقة الائتمانية وذلك في المادة (8/أولا) التي نصت على (يعاقب بالسحن المؤقت وبالغرامة لا تقل (10,000,000) عشرة ملايين دينار و لا تزيد على (15,000,000) خمسة عشر مليون دينار كل من ارتكب احد الأفعال:

---

(1)قانون العقوبات العراقي ، رقم 111 ، لسنة 1969 ، المادة (286).

ب- زور أو قلد أو اصطنع بنفسه أو بواسطة غيره بأي شكل من الإشكال بطاقة الكترونية أو ذكية بأي وسيلة تستخدم في تحويل النقود المحلية والأجنبية المتداولة داخل العراق أو استخدامها أو روج لها أو تعامل بها وهو يعلم بعدم صحتها[1].

وأن المادة (الثامنة/ ب) قد تناولت بشكل صريح موضوع تزوير البطاقة الالكترونية وذلك حين حددت الطرق التي يتم بها تغيير الحقيقة بالتزوير أو التقليد أو الاصطناع وسواء ارتكب هذه الأفعال بنفسه أو بواسطة غيره ، ويتضح أن المشرع في هذه المادة قد حرص على أيراد ألفاظ ذات معاني واسعة النطاق كما هو الحال حينما جاء بعبارة (بأي شكل من الأشكال) أي انه لم يحدد الطرق التي يتم بها التزوير أو التقليد أو الاصطناع.

وكذلك تكون العقوبة السجن لا تقل عن (10) عشر سنوات وبغرامة لا تقل عن (20,000,000)عشرين مليون ولا تزيد عن(30,000,000) ثلاثين مليون إذ كانت الأفعال المنصوص عليها في البند أولا من هذه المادة[2].

أ-تتعلق بحقوق الدولة أو القطاع العام أو الجهات التي تحقق النفع العام.

ب- ارتكبت من قبل موظف أو مكلف بخدمة عامة إثناء تأديته وظيفته أو بسببها.

ويتضح ان المشرع العراقي أيظاً شدد العقوبة في حالة أذا ارتكب الجاني جريمة تتعلق بحقوق الدولة أو القطاع العام ، أو إذا ارتكبت الجريمة من موظف أثناء تأديته عمله.

---

(1)مشروع قانون الجرائم المعلوماتية العراقي ، لسنة 2010.

(2)مشروع قانون الجرائم المعلوماتية العراقي ، لسنة 2010.

- ونص قانون الجرائم الإلكترونية الأردني ، رقم (27) لسنة 2015 في المادة (6) على ما يلي :" يعاقب كل من حصل قصداً دون تصريح عن طريق الشبكة المعلوماتية أو أي نظام معلومات على بيانات أو معلومات تتعلق ببطاقات الائتمان أو بالبيانات أو بالمعلومات التي تستخدم في تنفيذ المعاملات المالية أو المصرفية الإلكترونية بالحبس مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن (500) خمسمائة دينار ولا تزيد على (2000) الفي دينار[1].

ومن هذا النص أن المشرع الأردني جرم كل فعل يصدر من الجاني في الحصول على البطاقة الائتمانية قصداً أو عرقلة تنفيذ المعاملات المالية أو المصرفية بعقوبة نصت المادة عليه اعلاه ، ولم يكتفي بذلك المشرع الأردني حيث يعاقب أيظاً في المادة (7) بالأشغال الشاقة المؤقتة مدة لا تقل عن خمس سنوات وبغرامة لا تقل عن (5000) خمسة الالف دينار ولا تزيد عن (15000) خمسة عشر الف دينار ، أذا قام في الأفعال المنصوص عليها في المادة (6) إذا وقعت على نظام معلومات أو موقع الإلكتروني أو شبكة معلوماتية تتعلق بتحويل المالي ، أو بتقديم خدمات الدفع أو التقاص أو التسويات أو بأي من الخدمات المصرفية المقدمة من البنوك والشركات المالية.

أما المادة (8) من نفس القانون حيث تنص على مضاعفة العقوبة على الجرائم المنصوص عليها في المادة (6) من هذا القانون بحق كل من قام بارتكاب أي منها بسبب تأديته وظيفته أو عمله أو باستغلال أي منهما ، أي شدد العقوبة على كل شخص يرتكب مثل هذه الجرائم أثناء ممارسته لعمله الوظيفي الرسمي[2].

(1)قانون الجرائم الإلكترونية الأردني ، رقم 27 ، لسنة 2015، المادة (6).

(2)قانون الجرائم الإلكترونية الأردني ، رقم 27 ، لسنة 2015، المادة (8).

ويتضح مما سبق أن المشرع الفرنسي قصد إستيعاب التزوير العادي والإلكتروني من خلال وضع نص عام يمكن من خلاله المعاقبة على كل ما دخل تحت مضمونه من مفاهيم مع المحافظة على توحيد القوانين ضمن قانون العقوبات ، عكس التشريعات العربية التي ذكرناها والتي تحتي على قصور كبير في الإحاطة بهذه الجريمة.

الفصل الرابع

الإجراءات القانونية الخاصة لجريمة التزوير الإلكتروني و العقوبات المقررة لها

عند تطور الجرائم الإلكترونية أصبحت تشكل خطراً على أمن وسلامة الأفراد والدول ، وأصبح المجرم الإلكتروني أكثر خطورة و أكثر حركة وقوة عن ذي قبل ، ودخلت التقنيات الحديثة في المجال الإجرامي ، والتي ادت إلى تسهيل الكثير من النشاطات الإجرامية.

ولذلك لابد من وجود حماية خاصة لجريمة التزوير الإلكتروني وسنتطرق عنها في ثلاث مباحث في المبحث الاول سوف يتطرق الباحث إلى الإجراءات التنظيمية للحماية الخاصة لجريمة التزوير الإلكتروني وفي المبحث الثاني الإجراءات التطبيقية للحماية الخاصة لجريمة التزوير الإلكتروني ، والعقوبات المقررة لجريمة التزوير الإلكتروني في القوانين المقارنة .

المبحث الأول

الإجراءات التنظيمية الخاصة لجريمة التزوير الإلكتروني

تتألف الشبكات الإلكترونية من أجهزة الكمبيوتر المحلية المرتبطة بعضها ببعض بالشبكات الاقليمية والعالمية ، وهذا الربط مع استخدامه في الأنشطة الإجرامية الإلكترونية ، ساعد على ظهور العديد من المشكلات القانونية في مواجهة هذه الأنشطة الجرمية ، ومن أبرز هذه التحديات تلك التي تتعلق بالاختصاص والمعاينة و التفتيش والضبط والإثبات[1].

وتثار في هذا الصدد العديد من التساؤلات ، حول الأليات المفروض أتباعها في سبيل صياغة احكام قانونية التي تعمل على ردع مثل تلك الجرائم والتي من خلالها تًعطي للمحاكم الحق في النظر في القضايا الناشئة عن عمليات التزوير الإلكتروني. وهذا ما سيجري بحثه في هذا المبحث من خلال المطلبين الأول سيتحدث عن المبادئ المتعلقة بتحديد الاختصاص بالنظر في جرائم التزوير الإلكتروني والمطلب الثاني سيتطرق إلى المحاكم المختصة بالنظر في جرائم التزوير الإلكتروني.

المطلب الأول

المبادئ المتعلقة بتحديد الاختصاص بالنظر في جرائم التزوير الإلكتروني

يقابل التطور في المجال التكنولوجي سواء من ناحية الحياة العامة أم الخاصة وأعتماد الجميع عليه في سائر شؤونهم إستغلال الجناة لتلك التقنية في أرتكاب جرائمهم.

---

(1) بركات ، ميساء مصطفى ، (2009) ، جرائم التعدي على المعلوماتية الإتلاف و التزوير ، رسالة لنيل شهادة الماجستير ، جامعة بيروت العربية ، كلية الحقوق ، بيروت ، ص82.

فالقانون الجزائي بنصوصه الحالية (الشكلية والموضوعية) لا يكفي لإمكانية مواجهة تلك الصور المستحدثة من الجرائم الإلكترونية ، وذلك على الرغم من أن الكثير من هذه المجالات لا يمكن أن توفر النصوص العقابية التقليدية الحماية الكافية لها ، فكثير من التشريعات تعاني من قصور في تجريم هذا النوع من الجرائم بنصوص خاصة ومستقلة ، وأن وضعت نصوص خاصة لها، فأنها تكون ضيقة ولا تستوعب كل صور التجريم الخاصة بهذه الجرائم(1).

وهنا يدور التساؤل حول القانون الواجب التطبيق على الجرائم التي ترتكب عبر الإنترنت.

وإذا كانت القاعدة في تحديد الاختصاص هي في تطبيق مبدأ الأقليمية ، فهناك استثناءات ترد على هذه القاعدة ، وهي متعلقة بالمبادئ الأخرى ، كالعينية ، و الشخصية ، والعالمية.

وانطلاقاً مما تقدم ، سيُقسم هذا المطلب إلى أربعة فروع الأول مبدأ الإقليمية والثاني مبدأ الشخصية والثالث مبدأ العينية والرابع مبدأ العالمية.

الفرع الأول : مبدأ الإقليمية :

يعد مبدأ الإقليمية في تحديد الاختصاص من المبادئ المستقرة في قوانين دول العالم بأجمعها، لانه يرتبط ارتباطاً وثيقاً بسيادتها ، بل هو أهم مظاهر الدولة في سيادتها على إقليمها .

ويقصد بمبدأ الإقليمية ، تطبيق التشريع الجزائي على كل جرائم المرتكبة في إقليم الدولة، بصرف النظر عن جنسية الجاني أو المجني عليه سواء أكان وطنياً أم أجنبياً.

---

(1)مصطفى ، أحمد محمود ،(2010)، جرائم الحاسبات الإلية في التشريع المصري، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، ص221.

ونص عليه المشرع العراقي حيث نصت المادة السادسه من قانون العقوبات العراقي : " تسري أحكام هذا القانون على جميع الجرائم التي ترتكب في العراق وتعتبر الجريمة المرتكبة في العراق إذا وقع فيه فعل من الأفعال المكونة لها او إذا تحققت فيه نتيجتها او كان يراد أن تتحقق فيه[1].

وفي جميع الأحوال يسري القانون على كل من ساهم في جريمة وقعت كلها او بعضها في العراق ولو كانت مساهمته في الخارج سواء أكان فاعلاً أم شريكاً.

وقد أخذ المشرع الفرنسي بمبدأ الصلاحية الإقليمية أيضاً ، فتنص المادة 2/113 من قانون العقوبات على أنه :"يطبق القانون الفرنسي على الجرائم المرتكبة على إقليم الجمهورية وتعتبر الجريمة قد ارتكبت على إقليم الجمهورية ، إذا كان أحد عناصر الجريمة قد وقع على هذا الإقليم".

وقد أعتمد المشرع الأردني مبدا الإقليمية فنصت المادة السابعة من قانون العقوبات بقوله " تسري أحكام هذا القانون على كل من يرتكب داخل المملكة جريمة من الجرائم المنصوص عليها فيه "[2].

وتعتبر الجريمة مرتكبة في الأردن إذا تم على أرض هذه المملكة أحد العناصر التي تؤلف الجريمة أو أي فعل من افعال جريمة غير متجزءة أو فعل اشتراك أصلي أو فرعي.

من خلال النصوص السابقة ، يتبين أن العبرة هي في وقوع الجريمة كاملة او في جزء منها على إقليم إحدى هذه الدول ، أي السلوك أو النتيجة ، وقد جاءت اجتهادات المحاكم لتؤكد على الصلاحية الإقليمية في العديد من أحكامها.

ولذك تطرح الكثير من التساؤلات حول هل يمكن تطبيق النصوص القانونية السابقة على الجرائم المقترفة في الإقليم بواسطة الوسائل المستحدثة الإلكترونية؟.

---

(1)قانون العقوبات العراقي ، رقم 111 ، لسنة 1969 ، المادة (6).

(2)قانون العقوبات الأردني ، رقم 16 ، لسنة 1960، المادة (7).

إستناداً إلى النصوص السابقة ، فإنه يمكن توقيع العقوبة المقررة في هذه القوانين على كل من يقوم بإختراق أجهزة الكمبيوتر وعمل على تزوير البيانات أو الملفات الموجودة في إقليم معين ، وتحديد مكان الكمبيوتر لا اثر له على وقوع الجريمة في الإقليم الوطني ، باعتبار أن الفعل الإيجابي للمستخدم هو الذي يحدد الركن المادي لجريمة التزوير في الإقليم الأردني أو العراقي أو الفرنسي ، طالما أنه يمكن الأطلاع على المعلومات في الإقليم الوطني لكل منهما.

ولكن في أغلب الاحيان ، فإن هناك صعوبات مادية تحول دون تحديد مكان إرتكاب الجريمة الأصلية ، حيث ينعقد الاختصاص للقضاء الوطني نتيجة لتعقيد شبكة الأنترنت ، وتنوع طرق استخدامها ، ولذلك لابد من تحديد مكان ارتكاب الفعل ، لمعرفة ما إذا كان الفعل جرمياً أو لا ، وبغير ذلك لا يمكن محاكمة الفاعل و الشريك في حال عدم التمكن من تحديد مكان ارتكاب الجريمة[1].

الفرع الثاني : مبدأ الشخصية :

يقصد بمبدأ الشخصية وجوب سريان القانون الجزائي لكل دولة على رعاياها المتمتعين بجنسيتها أينما كانوا ، لمبدأ الشخصية وجهان : أحدهما إيجابي مؤداه تطبيق النص الجزائي على كل من يحمل جنسية الدولة ، ولو ارتكب جريمته خارج إقليمها ، أما الوجه الأخر السلبي فيعني سريان القانون الجزائي للدولة على الجرائم التي يكون المجني عليه فيها متمتعاً بجنسيتها ولو ارتكب الجريمة خارج إقليم الدولة[2].

حيث أن المشرع الفرنسي فقد اعتنق مبدأ الشخصية بوجهيه الإجابي و السلبي ، فجاء النص عليه بمقتضى المادة 1/113 من قانون العقوبات الفرنسي الذي يظهر الجانب الإيجابي واضحاً

(1)الصغير ، جميل عبد الباقي ، (2001) ، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت ، دار النهضة العربية ، القاهرة ، ص51.
(2)الصغير ، جميل عبد الباقي ، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت ، مرجع سابق ، ص 55.

من خلال ما جاء في سياق النص بأن " يطبق القانون الفرنسي على كل جناية يرتكبها فرنسي خارج فرنسا ، إذا كانت الوقائع المكونة لها معاقباً عليها في قانون الدولة التي إرتكبت فيها ، وتطبق أحكام هذه المادة ، حتى ولو كان المتهم قد اكتسب الجنسية الفرنسية بعد إرتكاب الواقعة المنسوبة إليه".

أما بالنسبة إلى الجانب السلبي لمبدأ شخصية النص الجزائي فقد تمثل بنص قانون العقوبات الفرنسي وفقاً للمادة 7/113 على أنه :" يطبق القانون الفرنسي على أية جناية ، وكذلك على أية جنحة يعاقب عليها بالحبس يرتكبها فرنسي أو أجنبي في الخارج ، إذا كان المجني عليه فرنسياً لحظة ارتكاب الجريمة"[1].

قد أخذ المشرع الأردني بل الجانب الإيجابي فقط حيث نصت المادة (9) من قانون العقوبات الأردني :"تسري أحكام هذا القانون على كل أردني و أجنبي – فاعلاً كان أو شريكاً– ارتكب خارج المملكة جناية أو جنحة مخلة بأمن الدولة ...."

وكذلك نصت المادة (10) منه ايضاً على إنه " تسري أحكام هذا القانون على كل أردني– فاعلاً كان أو شريكاً– ارتكب خارج المملكة جناية أو جنحة يعاقب عليها القانون الأردني.

من خلال النصوص السابق ، يتبين لنا أن مجال تطبيق القانون الفرنسي بوجهيه السلبي والإيجابي أوسع بكثير من مجال تطبيق القوانين في الدول التي تأخذ بالجانب الإجابي أو سلبي.

---

(1)بركات ، ميساء مصطفى ، جرائم التعدي على المعلوماتية الإتلاف و التزوير ، مرجع سابق ، ص86.

الفرع الثالث : مبدأ العينية :

يقصد بمبدأ العينية ، تطبيق قانون العقوبات الوطني للدولة على الجرائم التي تشكل مساساً بمصالح الدولة الجوهرية ، رغم عدم وقوعها على الإقليم الوطني ، وبصرف النظر عن جنسية مرتكبها ، وهذا الامتداد يستند إلى ما للدولة من حق ببسط سلطانها التشريعي على الجرائم التي تمس المصالح الأساسية ، خصوصاً حين لا تلقى هذه الجرائم اهتماماً من الدول التي وقعت على إقليمها[1].

وقد أعتمد المشرع العراقي مبدأ العينية حيث نصت المادة التاسعة من قانون العقوبات العراقي رقم 111 لسنة 1969 على أن (يسري هذا القانون على كل من ارتكب خارج العراق جريمة ماسة بأمن الدولة الخارجي أو الداخلي أو ضد الجمهورية ...). ويفهم من هذا النص أن قانون العقوبات العراقي لم يشترط في مرتكب الجريمة الواقعة على سلامة الدولة أو استقلالها السياسي في الخارج أن يكون عراقي الجنسية ، فقد ساوى بين العراقي والأجنبي في الحكم لأنه جاء بصيغة التعميم (كل من) وهذا الاتجاه هو السائد في قوانين الدول الأوربية ، و أساس الماساواة بين العراقي والأجنبي هو الحماية و المحافظة على أمن الدولة وسلامتها بل وحمايتها ، مما يوجب عدم تقبل أي تفرقة بينه وبين المواطن.

وكذلك أعتد المشرع الأردني أيضاً بمبدأ العينية في المادة التاسعة على أنه :" تسرى أحكام هذا القانون على كل اردني أو اجنبي – فاعلاً كان أو شريكاً محرضا كان متدخلا– ارتكب خارج

---

(1)عالية ، سمير ، (1996) ، أصول قانون العقوبات ، القسم العام ، الطبعة الأولى ، المؤسسة الجامعية للدراسات والنشر و التوزيع ، بيروت ، ص126.

المملكة جناية او جنحة مخلة بأمن الدولة او قلد ختم الدولة او قلد نقودا او زور اوراق النقد او السندات المصرفية الأردنية أو الأجنبية المتداولة قانونا او تعاملا في المملكة.

وقد أخذ المشرع الفرنسي بمبدا العينية ، فنصت المادة 10/113 من قانون العقوبات الفرنسي الجديد ، على أنه :" يطبق القانون الفرنسي ، على كل جنايات و الجنح التي ترتكب في الخارج ، والتي تشكل أعتداء على المصالح الأساسية للأمة ، وكذلك جرائم تقليد أختام الدولة وتزويرها، وتزييف العملة المعدنية أو الورقية أو السندات العامة ، وعلى أية جناية أو جنحة ترتكب ضد أعضاء البعثات الدبلوماسية أو أماكنهم ، أو القنصلية الفرنسية في الخارج"[1].

وبتطبيق تلك النصوص على جرائم الإلكترونية . يمكن القول : إن هناك العديد من الجرائم المتعلقة بالتزوير الإلكتروني يمكن أن تندرج ضمن هذا المبدأ ، بغض النظر عن جنسية الفاعل ، حتى لو ارتكب الفعل خارج إقليم هذه الدولة ، لذلك تبرز أهمية التعاون الدولي لمكافحة الجرائم الإلكترونية.

الفرع الرابع : مبدأ العالمية :

يقصد بمبدأ العالمية سريان قانون عقوبات الدولة التي يكون فيها الفاعل على الجرائم التي يرتكبها الفاعل خارج إقليم الدولة ، بغض النظر عن مكان وقوع الجريمة أو جنسية الفاعل أو المجني عليه.

وقد أخذ المشرع العراقي بمبدأ العالمية تحت مسمى الاختصاص الشامل حيث نصت المادة 13 على انه :" في غير الأحوال المنصوص عليها في المواد 9 و 10 و 11 تسري أحكام هذا

---

(1)بركات ، ميساء مصطفى ، جرائم التعدي على المعلوماتية الإتلاف و التزوير ، مرجع سابق ، ص88.

القانون على كل من وجد في العراق بعد أن ارتكب في الخارج بوصفه فاعلا او شريكا جريمة من الجرائم التالية: تخريب او تعطيل وسائل المخابرات والمواصلات الدولية..ألخ [1].

وكذلك أخذ المشرع الأردني في المادة العاشرة في فقرة (4) منه على أنه :" تسري أحكام هذا القانون :

4- على كل أجنبي مقيم في المملكة الأردنية الهاشمية ، فاعلاً كان أو شريكاً محرضاً أو متدخلاً ، ارتكب خارج المملكة الأردنية الهاشمية جناية أو جنحة يعاقب عليها القانون الأردني. إذا لم يكن استرداده قد طلب أو قبل[2].

ويمكن تبرير الأخذ بهذا المبدأ في مجال الانترنت ، إستناداً إلى ان هذه الشبكة قد تخطت كل الحواجز المادية ، فأصبح المجال أوسع ، وأسهل للمجرم الإلكتروني لارتكاب العديد من الجرائم بواسطتها و الفرار من العقاب ، فمهمة هذا المبدأ هو المساعدة على عدم إفلات المجرم من فعله ، حتى لو لم يكن على إقليم الدول التي يحمل جنسيتها .

المطلب الثاني

المحاكم المختصة بالنظر في جرائم التزوير الإلكتروني

تطورت استخدامات التقنية في كافة أشكال الحياة، خصوصا بعد أن بدأ استخدامها في العالم ، وانتشار استخدام الحاسب الآلي في المنزل والمكتب، واتصال الأجهزة بعضها مع بعض

(1)قانون العقوبات العراقي ، رقم 111 ، لسنة 1969 ، المادة (13).
(2)قانون العقوبات الأردني ، رقم 16 ، لسنة 1960 ، المادة (10).

عبر الشبكات الداخلية للمنشآت والشبكات المحلية والدولية من خلال الشبكة العنكبوتية، وتناقل البيانات والمعلومات خلالها.

ومع وجود هذا العالم الافتراضي انتقلت إليه الجرائم التي كانت فيما مضى لا يمكن تطبيقها إلا على أرض الواقع لتتم عبر تلك الشبكات على ساحات العالم الافتراضي ، مما يجعل من تطبيق القانون الجزائي الدولي على شبكة الإنترنت ، يواجه صعوبات قانونية متعددة.

فانتقال المعلومة ضمن شبكة الإنترنت بين مختلف دول العالم ، قد يؤدي إلى تطبيق تراكمي محتمل لجميع قوانين الدول المتصلة بهذه الشبكة دفعةً واحدة[1].

وهذا الأمر طرح إشكالية قانونية ، تتمثل في كيفية تحديد المحكمة المختصة بالنظر بالنزاع الذي قد يثور في هذه الحالة ، وهذا ما استوجب البحث عن معايير التي يمكن أن تنبثق عنها الحلول المناسبة لهذه الإشكالية ، فتباينت بناءً على ذلك المعايير التشريعية التي اعتمدت في تحديد المحاكم المختصة بالنظر بالجرائم الإلكترونية ، وهو الأمر الذي سيجري بحثه من خلال الفروع وحيث سنتطرق في الفرع الأول عن معيار الاختصاص المكاني و في الفرع الثاني عن معيار القانون الأكثر ملاءمة وفي الفرع الثالث معيار الضرر المرتقب.

---

(1)عيسى ، طوني ميشال ، (2001) ، التنظيم القانوني لشبكة الإنترنت ، الطبعة الأولى ، منشورات صادر الحقوقية ، بيروت ، ص433.

الفرع الأول : معيار الاختصاص المكاني :

تتبع أغلب التشريعات في تحديد الاختصاص المكاني ثلاثة ضوابط هي : مكان وقوع الجريمة، أو محل إقامة المتهم ، أو مكان إلقاء القبض عليه ، وفي حال اجتماع أكثر من ضابط ، تكون المحكمة التي ترفع إليها الدعوى أولاً هي المختصة مكانياً بالنظر في الدعوى[1].

وقد أعتبر البعض أنه يجب أن ينظر إلى أختصاص محل ارتكاب الجريمة ، كاختصاص رئيسي يقدم على غيره ، ويتبعه اختصاص محل الإقامة ، ثم اختصاص مكان إلقاء القبض على المتهم أو الجاني[2].

بالنسبة إلى الجرائم الإلكترونية ، فإن السلوك و النتيجة يتماثلان في جريمة . ومن ثم فإن محاكم مكان النشاط الجرمي ومكان النتيجة تكون مختصة أيضاً . وعلى ذلك ، في حال إرسال الفيروس الإلكتروني إلى مكان ، وتدمير المعلومات في مكان آخر ، وتحقيق النتيجة في مكان أخر و إلقاء القبض على الجاني في مكان ثالث ، فإن الاختصاص ينعقد لمحاكم احدى هذه الأماكن[3].

وقد اعتمدت العديد من الدول معيار الاختصاص المكاني كالولايات المتحدة الأمريكية ، فقد أعطى القانون الأمريكي الاختصاص للمحاكم الأمريكية على المستوى الفيدرالي للنظر في كل جريمة يرتكبها أمريكي أو أجنبي ، إذا كان مقيماً داخل الولايات المتحدة ، أو في المناطق التابعة

---

(1)الصيفي ، عبد الفتاح ، دون سنة طباعة ، أصول المحاكمات الجزائية ، دار النهضة العربية ، مصر ، ص120.
(2)النقيب ، عاطف ، (1986) ، أصول المحاكمات الجزائية ، دراسة مقارنة ، منشورات عويدات ، بيروت ، ص124.
(3)الصغير ، جميل عبد الباقي ، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت ، مرجع سابق ، ص62.

لها ، أو التي تدخل ضمن حدودها الجغرافية أو السياسية أو إرتكب أحد أفعال الجريمة في الولايات المتحدة[1].

ولذلك إن جرائم الإنترنت ، لا تحدّها حدود خلافاً للجرائم التقليدية المعروفة ، الأمر الذي يجعلها في كثير من الأحيان تستعصي على الخضوع لنصوص القانونية التي تحكم مسألة الاختصاص المكاني ، ومن ثم ، فإن الطبيعة الخاصة لهذا الصنف من الجرائم الإلكترونية تتطلب تجاوز النصوص والمعايير التي طرحها الفقه للتغلب على مشكلة تنازع الاختصاص ، والعمل على تبني حلول أكثر مرونة تأخذ في الحسبان النطاق الجغرافي لهذه الجرائم وسهولة ارتكابها وآلية اقترافها والتخلص من آثارها وما إلى ذلك من اعتبارات يفرضها الطابع التقني المتطور لها .

وقد اصدرت العديد من الدول العربية قانونين تعاقب على الاعمال المرتكبة عبر الأنترنت وفقاً للاختصاص المكاني ، ومنها دولة الإمارات العربية المتحدة ،

الفرع الثاني : معيار القانون الأكثر ملاءمة :

تسبب جرائم الإلكترونية التي ترتكب بواسطة الإنترنت أضراراً كبيرة قد تتفاوت بين دولة وأخرى ، مما يفرض التوسع في تفسير قاعدة اختصاص محكمة وقوع الفعل ، ليكون الاختصاص للدولة الأكثر تعرضاً للضرر ، مع التركيز على مبدأ التنازل للمحكمة أو التخلي عن الاختصاص[2] .

---

(1)بركات ، ميساء مصطفى ، جرائم التعدي على المعلوماتية الإتلاف و التزوير ، مرجع سابق ، ص90.

(2)عيسى ، طوني ميشال ، التنظيم القانوني لشبكة الإنترنت ، مرجع سابق ، ص447.

بخلاف ذلك ، فإن اعطاء الاختصاص لقانون دولة ما لمجرد إمكانية الوصول إلى معلومة من هذه الدولة أو تلك ، أصبح غير كافٍ من الناحية القانونية لاعلان اختصاص هذه الدولة أو تلك.

والهدف من المناداة بهذا المعيار ، هو البحث عن القانون النموذجي الأكثر ملاءمة للاختصاص في نظر المنازعة المطروحة ، ومن أمثلة ذلك ، ما أصدرته إحدى المحاكم الأمريكية، التي اعتبرت فيه ، أنه لا يمكن الارتكاز إلى مجرد النفاذ ، أو الاتصال بهذا الموقع أو المورد انطلاقاً من الأراضي الأمريكية ، حتى ينعقد الاختصاص لها للنظر في النزاع المعروض أمامها[1].

الفرع الثالث : معيار الضرر المرتقب :

طرح المعيار المرتقب أول مرة في مسودة مشروع اتفاقية لاهاي الدولية ، من أجل المساهمة في الحد من حالات الافراط في الاختصاص القضائي المحتمل للمحاكم في مجال نشر المعلومات عبر شبكة الإنترنت.

وقد قدم مجلس العدلي الأوربي تفسيراً خاصاً ، بشأن مفهوم قاعدة اختصاص محل وقوع أو حدوث الفعل الضار ، وبذلك بالتأكيد على حق المتضرر ، باللجوء حسب خياره إلى محكمة محل ارتكاب الفعل ، أو إلى محل وقوع الضرر ، ولكن مع إضافة قيد هام ، في حالة لجوء المتضرر إلى محكمة محل وقوع الضرر ، يقتضي حجب إختصاص هذه المحكمة إذا أثبت

(1)بركات ، ميساء مصطفى ، جرائم التعدي على المعلوماتية الإتلاف و التزوير ، مرجع سابق ، ص92

المدعي عليه أنه لم يكن قادراً على توقع الضرر بصورة معقولة ، وأن الفعل أو الامتناع كان من شأنه إحداث ضرر مماثل في دولته[1].

وقد طبق هذا المعيار في بعض الدول ومنها فرنسا ، حيث أصدرت محكمة استئناف باريس في عام 1999 ، قراراً اعتبر صراحة أن طبيعة العالمية الخاصة بشبكة الإنترنت ، يجب ألا تؤدي إلى تطبيق محتمل لجميع قوانين الموجودة ، بل إلى تطبيق القانون ذي الصلة مع مبدأ موضوعي هو توقيع المسؤول للمحتوى الضار الذي ينشره[2].

ويرى الباحث أن المحكمة المختصة في النظر في الجرائم الإلكترونية ومن ضمنها جريمة التزوير الإلكتروني تعتمد اولاً على المعيار الاختصاص المكاني من حيث وقوع جريمة أو محل الأقامة المتهم أو مكان إلقاء القبض عليه ، لكن لا يكفي الاختصاص المكاني وحده بل لابد النظر إلى معايير أخرى وخصوصاً وأن جريمة التزوير الإلكتروني لا يحدها حدود وترتكب عبر الشبكة الإلكترونية فلهذا لابد أن ينظر إلى معيار الضرر المرتقب من أجل حل هذا النزاع الحاصل في المحكمة المختصة في مثل تلك الجرائم.

---

(1)إتفاقية لاهاي لعام 1999 ، المادة (10)

(2)عيسى ، طوني ميشال ، التنظيم القانوني لشبكة الإنترنت ، مرجع سابق ، ص449 وما بعدها.

المبحث الثاني

الاجراءات التطبيقية الخاصة لجريمة التزوير الإلكتروني و العقوبات المقررة له

بعد البحث في الاجراءات التنظيمية للحماية الخاصة بجريمة التزوير الإلكتروني سواء من حيث المبادئ المتعلقة بتحديد الاختصاص للنظر في هذه الجريمة ، أو من حيث المحاكم المخولة، لذلك يجب أيضاً الانتقال إلى بحث في الجانب العملي من هذا الموضوع ، وهو ما يتمثل في التطبيقات التي تقوم بها الجهات العدلية و القضائية في سبيل مكافحة جريمة التزوير الإلكتروني[1].

على ذلك فقد قسمنا هذا المبحث الى مطلبين حيث سيتطرق الباحث في المطلب الأول عن دور الضابطة العدلية في مواجهة جرائم الكمبيوتر وفي المطلب الثاني دور القاضي في تقييم الأدلة الخاصة بجرائم الكمبيوتر أما المطلب الثالث تتناول الدراسة فيه عن العقوبات المقررة في التشريعات المقارنة.

المطلب الأول

دور الضابطة العدلية في مواجهة جرائم الكمبيوتر

بعد ان أصبح المجتمع الإلكتروني حقيقة لا لبس فيه ، إثر اعتماد المجتمعات في تسيير شؤونها على تقنيات الكمبيوتر والمعلومات ، باتت الحاجة ملحة لوضع قواعد جزائية موضوعية جديدة ، تستوعب هذا الكم الهائل من المعلومات ، وتكفل مجابهة الأشكال المستخدمة للجرائم الناشئة عن إساءة استخدام هذه التقنية[2].

---

(1)بركات ، ميساء مصطفى ، جرائم التعدي على المعلوماتية الإتلاف و التزوير ، مرجع سابق ، ص94.

(2)بركات ، ميساء مصطفى ، جرائم التعدي على المعلوماتية الإتلاف و التزوير ، مرجع سابق ، ص94.

هذا الواقع يستوجب التطرق إلى دور الضابطة العدلية ، من خلال عرض الأساليب الفنية المعتمدة من قبل الأجهزة للتعامل مع جرائم و مواجهتها ، بأقصى قدر ممكن من الفعالية.

ولذلك سيتم تقسين هذا المطلب إلى فرعين حيث سيتطرق الباحث في الفرع الأول إجراءات الضابطة العدلية في معاينة جهاز الكمبيوتر وفي الفرع الثاني إجراءات الضابطة العدلية في تفتيش والضبط الأدلة الكمبيوتر.

الفرع الاول : إجراءات الضابطة العدلية في معاينة جهز الكمبيوتر :

تعتبر مرحلة المعاينة من أول و أهم المراحل الضرورية في كشف الجرائم ، حيث يبرز دور الضابطة العدلية في معاينة المكان الذي ارتكبت فيه الجريمة ، ولكن في إطار الجريمة الإلكترونية فإن مسرح الجريمة هو جهاز الكمبيوتر [1].

ويتكون جهاز الكمبيتور من مكونات مادية وأخرى معنوية لذلك فإن المعاينة لابد أن تشمل كلا النوعين وهذا ما سنبينه في النقطتين التاليتين :

اولاً:المعاينة على الجرائم الواقعة على المكونات المادية للكمبيوتر :

يقصد بالمعاينة في معناها الواسع ، تلك الرؤية أو المشاهدة بالعين لأي أمر ، وتكاد تتركز غالبية تعريفات المعاينة حول كونها إجراء يهدف إلى إثبات حالة شيء أو شخص أو مكان ، وذلك عن طريق الرؤية و الفحص المباشر [2].

---

(1)بركات ، ميساء مصطفى ، جرائم التعدي على المعلوماتية الإتلاف و التزوير ، مرجع سابق ، ص95

(2)البرادعي ، أحمد بن عبد الله ، (1995) ، معاينة الجريمة بين النظرية و التطبيق ، مطابع ينبع الحديثة ، المملكة العربية السعودية ، ص13.

ويصفها البعض الاخر وصفاً أكثر دقة بتعريفه بأنها :"إثبات لحالة الأماكن و الأشخاص وكل ما يفيد في كشف الحقيقة"[1].

وتعد المعاينة الخطوة الاولى في مراحل ملاحقة الجاني و القبض عليه ، وهي خطيرة بطبعها إذا نفذت بشكل غير صحيح حيث تؤدي إلى نتائج خاطئة ، وإلى إتساع المسافة بين العدالة و المجرم.

ويجب على الضابط العدلي وضع يده على الأدلة المادية التي تفيد التحقيق ، وكذلك وضع الأختام في الأماكن التي أجريت فيها المعاينة متى وجد فيها أثاراً أو أشياء تفيد في كشف الحقيقة ، ويجوز لها تعيين حراس على هذه الأماكن مع ضرورة إخطار النيابة بهذه الاجراءات[2].

أما عن مدى صلاحية مسرح جرائم الكمبيوتر للمعاينة ، فإن جرائم الاعتداء على أنشطة الكمبيوتر و شاشة العرض الخاصة به ومفاتيح التشغيل وغيرها ، لا تثير أدنى صعوبة للتقرير بصلاحية مسرح الجريمة ، الذي يحوي هذه المعدات لمعاينتها من قبل الضابط العدلي ، وكشف كل الأثار و الأدلة الناجمة عن تنفيذ الجريمة ، ولابد من القول أن سرعة الانتقال إلى مسرح الجريمة يعد أهم إجراءات التحقيق ، لما يترتب عليه من تسهيل مهمة المحقق في معاينة المسرح ، وسماع الشهود قبل أن تضيع معالم الجريمة[3].

---

(1)عبد الستار ، فوزية ، (1986) ، شرح قانون الاجراءات الجنائية ، دار النهضة العربية ، القاهرة ، ص332.

(2)طنطاوي ، إبراهيم حامد مرسي ، (1997) ، سلطات مأمور الضبط القضائي ، دراسة مقارنة ، أطروحة لنيل شهادة الدكتوراه ،المكتبة القانونية ، القاهرة ، ص293.

(3)عبد الستار ، فوزية ، شرح قانون الاجراءات الجنائية ، مرجع سابق ، ص321.

ثانيا: المعاينة على الجرائم الواقعة على مكونات المعنوية للكمبيوتر :

إذا كان رجال الضابطة العدلية لا يواجهون أية صعوبة في معاينتهم لمسرح الجريمة الواقعة على المكونات المادية بجهاز الكمبيوتر ، إلا أن الصعوبات الحقيقية تظهر عندما تكون الجريمة واقعة على برامج الكمبيوتر وما يحتويه من بيانات ، أي عندما يقوم المجرم الإلكتروني بأعمال تتعلق بالتعدي على كينونة جهاز الكمبيوتر ، أي القيام بإتلاف للبرامج أو تزوير المحررات الإلكترونية ، وهذه الصعوبات تحول دون فعالية المعاينة أو فائدتها[1].

فالجرائم التي تقع على الكمبيوتر تكون مخفية في أكثر صورها ، ولا يلحظها المجني عليه أو يدري بوقوعها والامعان في حجب السلوك و إخفائه عن طريق إرسال الفيروسات أو التلاعب بالبيانات ليس عسيراً ، وخصوصاً مع توافر الخبرة الفنية و التقنية العالية لدى مرتكبها.

كما إن غياب الدليل المرئي ، يتمثل في أن المعلومات مسجلة بصورة مرمزة ، لا يمكن للإنسان قراءتها ، و إن كانت قابلة للقراءة من قبل الكمبيوتر نفسه ، إلا أن المجرم لا يترك أي أثر، مما يقطع غالبا كل صلة بين المجرم و جريمته ، ويحولف دون كشف شخصية مرتكبها أو ضبط المستند المزور مثلاً[2].

بالإضافة إلى ذلك ، فإن المجرم الإلكتروني قد يُصعب عملية التفتيش المتوقع عن الآدلة التي قد تدينه ، بقيامه بالعديد من التدابير الأمنية التي يضر بها من حوله ، كأستخدام كلمات سر للوصول إليها ، أو منع الاطلاع على البيانات من خلال التشفير مثلاً ، ومن صعوبات الاضافية

---

(1)طنطاوي ، إبراهيم حامد مرسي ، سلطات مأمور الضبط القضائي ، مرجع سابق ، ص 295.

(2)بركات ، ميساء مصطفى ، جرائم التعدي على المعلوماتية الإتلاف و التزوير ، مرجع سابق ، ص98.

في هذا المجال يمكن ذكر سهولة محو الدليل أو تدميره في زمن قصير جداً ، فضلاً عن سهولة تنصله من المسؤولية[1].

ولابد من الأشارة إلى أنه حفاظاً على مسرح الجريمة ، يوصى في هذا الإطار على ما يلي :

أ- تصوير الكمبيوتر وما يتصل به من أجهزة بدقة تامة ، و إلتقاط صورة لأجزائه الخلفية وسائر ملحقاته.

ب-عدم التسرع في نقل أية مادة إلكترونية من مكان وقوع الجريمة ، قبل إجراء اختبارات للتاكد من خلو المحيط الخارجي لموقع الكمبيوتر من أية حالات للقوى المغنطيسية خشية إتلاف البيانات المخزنة

الفرع الثاني : إجراءات الضابطة العدلية في التفتيش و الضبط لأدلة الكمبيوتر :

يشكل ظهور هذه الأنماط الجديدة من الجرائم ، عبئاً ثقيلاً على عاتق أجهزة الضابطة العدلية ، نظراً إلى ما تتطلبه هذه الجرائم من الكفاءة و المعرفة و القدرة على كشف الغموض المحيط بها ، و التعرف إلى مرتكبيها ، وذلك يتم من خلال السرعة في التفتيش وضبط الأدلة ، لذلك سوف نقسم هذا الفرع إلى نقطتين مهمتين وهي :

(1)رستم ، هشام محمد فريد ، (1999) ، الجرائم المعلوماتية ، أصول التحقيق الجنائي الفني و آلية التدريب التخصصي للمحققين ، مجلة الأمن و القانون ، السنة السابعة ، العدد الثاني ، ص87.

اولاً : تفتيش مسرح جرائم الكمبيوتر :

يمكن تعريف التفتيش بأنه : " إجراء من إجراءات التحقيق ، يقوم به موظف مختص وفقاً للاجرءات المقررة قانوناً في محل يتمتع بالحرمة ، بهدف الوصول إلى أدلة مادية لجناية أو جنحة تحقق وقوعها ، لإثبات ارتكابها أو نسبتها إلى المتهم"[1].

وإستناداً إلى ذلك يتميز التفتيش بعدة خصائص : فهو إجراء من إجراءات التحقيق ، يهدف إلى بحث عن ادلة مادية لجناية أو جنحة تحقق وقوعها ، وموضوعة في محل يتمتع بحرمة المسكن أو الشخص ، ولابد أن يتم ذلك وفق الاجراءات القانونية المقررة ، ووفقاً للضوابط التي وضعها المشرع.

ثانياً : ضبط ادلة الكمبيوتر :

يقصد بالضبط في القانون الإجراءات ، وضع اليد على شيء يتصل بجريمة وقعت ، ويفيد في كشف الحقيقة عنها وعن مرتكبها، وهو من ناحية محله ولا يرد إلا على الأشياء المادية ، أما الأشياء المعنوية فلا تصلح محلاً لوضع اليد ، ويقصد بالضبط هنا الضبط القضائي ، الذي يهدف إلى الحصول على الأدلة المتصلة بالتفتيش لمصلحة التحقيق لإثبات واقعة معينة[2].

والضبط لا يعني أنه لا يقع إلا نتيجة تفتيش ، إذ من الممكن أن يكون الضبط نتيجة لمعاينة ، كما أنه يجوز أن تضبط أشياء قدمها الشهود ، أو المتهمون باختيارهم ،وكذلك يجوز للمحقق أن يطالب أحد الأفراد بتسليم شيء في حوزته ، ويمكنه إلزامه في ذلك[3].

---

(1)طنطاوي ، إبراهيم حامد مرسي ، سلطات مأمور الضبط القضائي ، مرجع سابق ، ص743.

(2)الشاوي ، توفيق ، (1954) ، فقه الاجراءات الجنائية ، دار الكتاب العربي ، القاهرة ، ص491.

(3)رستم ، هشام محمد فريد ، الجرائم المعلوماتية ، مرجع سابق ، ص93.

وللمحقق أن يأمر بضبط الشيء بعد تقديمه ، ذلك أن الامتناع عن تقديم الشيء في هذه الحالة يؤدي إلى فرض عقوبة الامتناع عن الشهادة.

ولا يتوقف ضبط جهاز الكمبيوتر على المكونات المادية فقط ، بل يمتد إلى مختلف أجزاء النظام أي أنه يمتد إلى معطيات و البيانات و البرامج المخزنة في داخله ، أي إلى أشياء ذات صيغة معنوية معرضة بسهولة للتغيير.

أما فيما يخص ببرامج الكمبيوتر ، بما يتضمنه من معلومات و بيانات ، فإن الصعوبة تظهر في حال إستخدام وسائل فنية في إتلافه وتغيير ما فيه من بيانات و معلومات عن طريق إختراقه بفيروس ، وتكمن الصعوبة في هذه الحالة في قلة الخبرة لدى ضابط العدلية ، بإعتبارها الجهة المختصة بالضبط ، أما الصعوبة الثانية فتتمثل في أن عملية الضبط تواجه صعوبة في الحالات التي تكون فيها البيانات مخزنة في نظم معالجة مركزية في الكمبيوتر ، ضمن شبكة معلومات كبيرة ، في هذه الحالة ، فإن صياغة شرط يعطي للمحقق إمكانية ضبط هذا النظام الشبكي بأكمله ، وعزله عن البيئة الإلكترونية المحيطة به لا يعد تشريعاً حقيقياً لمبدأ التناسب لما فيه من مساس بحقوق الغير في النظام محل الضبط(1).

خصوصاً ان جريمة الإلكترونية هي من الجرائم المستحدثة ، التي لا تترك شهوداً يمكن استجوابهم ، ولا أدلة مادية يمكن فحصها ، من هنا تكمن الصعوبة في كشف عن هذه الجرائم.

لذلك فإن مواجهة الجرائم الإلكترونية يلتزم اتخاذ إجراءات قد تتجاوز المفاهيم المستقرة التقليدية، وذلك لما تتسم به هذه الجرائم من حداثة في الأسلوب، وسرعة في التنفيذ، وسهولة في إخفائها، وقدرة على محو آثارها، وقد أثبت الوقائع العملية أن هناك جرائم قد أرتكبت على مرأى من

---

(1)أحمد ، هلالي عبد الله ، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي ، مرجع سابق ، ص201.

رجال الضبط ومسمعهم ، بل قام هؤلاء بتقديم المساعدة لهم دون قصد و عن جهل ، مثلما حدث عندما طلبت إحدى دوائر الشرطة في الولايات المتحدة من شركة تعرضت للقرصنة أن تتوقف عن تشغيل الكمبيوتر الخاص بها ، لتتمكن من وضعه تحت المراقبة بهدف كشف مرتكب الجريمة ، ونتيجة ذلك أتلف ما كان قد سلم من الملفات والبرامج(1).

المطلب الثاني

دور القاضي في تقييم الادلة الخاصة بجرائم الكمبيوتر

وتزداد الصعوبة في الدور الذي يلعبه القاضي في مواجهة حالات التعدي اذا كانت تمس مصالح المجتمع والأفراد على حد سواء ؛ ويزداد الأمر تعقيداً اذ يتوجب على القاضي الجزائي الإلمام ببعض المعرفة الفنية للكمبيوتر وأنظمة وما يستجد في هذا المضمار، حيث تحال القضية موضوع الدعوى الى القاضي للنظر فيها ،بهدف تحديد آلية عمله في القضية ، واستخراج الأحكام التي تتناسب معها وتقييم أدلة الجريمة ، وتقدير مدى مشروعية الدليل المستمد من الإنترنت.

لذلك سنقسم هذا المطلب على ثلاث فروع حيث سيتناول الفرع الأول عن نظام الأدلة القانونية و الفرع الثاني يتناول نظام الإقتناع الذاتي للقاضي أما الفرع الثالث يتناول نظام الإثبات المختلط.

الفرع الاول: نظام الأدلة القانونية :

بموجب هذا النظام يتقيد القاضي في حكمه بالإدانة او البراءة بأنواع معينة من الأدلة المحددة مسبقا من قبل المشرع ، بغض النظر عن اقتناعه او عدم اقتناعه بصحة ثبوت الواقعة او عدم ثبوتها ، إذ يقوم اقتناع المشرع بصحة الإسناد أو عدم صحته مقام اقتناع القاضي.

(1)أحمد ، هلالي عبد الله ، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي ، مرجع سابق ، ص203.

يقوم اليقين القانوني على افتراض صحة الدليل ، بغض النظر عن حقيقة الواقع أو اختلاف ظروف الدعاوى ، ومن هنا ، فإن القاضي يحكم في الدعوى المطروحة أمامه طالما توافرت الشروط القانونية في الدليل المطروح في الدعوى ، حتى لو كان مقتنع بادانته ، واذا لم تتوافر هذه الأدلة ، التزام القاضي بتبرئة المتهم ، بصرف النظر عن اعتقاده الشخصي ، إي لو كان مقتنعاً بإدانته [1].

فالمشرع هو الذي يقوم بالدور الإيجابي في عملية الإثبات في الدعاوى ، أما دور القاضي فيتمثل في مجرد التحقيق في توافر الأدلة وشروطها القانونية وشرح حججه ، أما عن موضوع الأدلة التي تكون من ضمن الجرائم الإلكترونية وحول قبول الأدلة في صورة مخرجات للكومبيوتر كأداة صالحة للإثبات امام القضاء، وذلك باعتبار أن "الإنشاءات الإلكترونية والنبضات الممغنطة التي تعتمد عليها إجهزة الكمبيوتر ليست مرئية بالعين المجردة، وبالتالي لايستطيع القاضي رؤية الدليل الأصلي، ومايقدم إليهم هو نسخ لأصول ممايجعله ثانوياً لا أصلياً[2].

لكن يبقى أن القاضي ضمن هذا نظام لا يستطيع أن يحكم حسب إقتناعه الشخصي يبقى مقيد بنطق الحكم حسب الأدلة التي حصرها المشرع.

الفرع الثاني : نظام الإقتناع الذاتي للقاضي

يعد نظام الإقتناع الذاتي للقاضي من أكثر الأنظمة شيوعاً ، ويقوم هذا النظام على عدم تحديد الأدلة مسبقاً التي يجب أن يستند إليها القاضي في إصدار حكمه ، فقد نصت على المادة

---

(1)سرور ، أحمد فتحي ، (1995) ، الشرعية الدستورية وحقوق الإنسان في الاجراءات الجنائية ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، ص746.

(2)عفيفي كامل عفيفي ، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون ، مرجع سابق ، ص386.

1\302 من قانون الاجراءات الجزائية المصرية بقولها "يحكم القاضي وفق العقيدة التي تكونت لديه بكامل حريته"، وقد فتح هذا النص الباب على مصراعيه أمام القاضي الجزائي ، وبالتالي أضحى يتمتع بسلطة واسعة من ناحية قبول الأدلة ، وهو غير مطلب بدليل معين، ففي كل الأحوال تخضع الأدلة لتقدير القاضي[1].

وإستناداً إلى ما سبق، يتضح أنه في ظل هذا المبدأ لا وجود لأدلة يحظرها المشرع على القضاء أو يقبلها ، إذ لا وجود لمانع يحول دون قبول مخرجات الكمبيوتر أمام القضاء الجزائي كأدلة لإثبات وقائع الدعوى المنظورة أمامه، وقد استقرت أحكام المحاكم الفرنسية على أنه: " ما كان له من التسجيلات الممغنطة قيمة الدلائل... يمكن ان يكون صالحاً لتقديمه للقضاء الجنائي، وأنه إذا قررت محكمة الموضوع وفقآ لاقتناعها الذاتي ، وقواعد القانون العام ما استندت الى النيابة من قرائن... بشأن خطأ سائق سيارة منسوب إليه تجاوز السرعة الثابتة بمساعدة جهاز آلي... ودون أن يكون السائق قد سئل ، فإنها لا تكون ملزمة بتحديد ما استندت إليه من عناصر الواقعة في تأسيس قناعتها " [2].

الفرع الثالث : نظام الإثبات المختلط :

يعتقد البعض أن نظام الاثبات المختلط هو مزيج بين نظامي الأدلة القانونية ونظام الإثبات المطلق في محاولة لجمع مزاياهما وتلافي مساوئهما.

---

(1)الغريب ، محمد عيد ، (1997) ، حرية القاضي الجنائي في الإقتناع اليقيني و أثره في تسبيب الأحكام الجنائية ، الطبعة الأولى ، النسر الذهبي للطباعة والنشر ، القاهرة ، ص8.

(2)رستم ، هشام محمد فريد ، الجرائم المعلوماتية ، مرجع سابق ، ص156.

وهذا الرأي يطابق الحقيقة ، إذ أن هذا النظام قائم على تحديد المشرع مسبقاً لأدلة الإثبات التي يجوز للقاضي الاستناد إليها عند إصداره حكمه في الدعوى التي ينظر فيها، مع حقه في تقييم كل دليل على حدة وتقدير مدة كفايته للحكم بالإدانة ، أي أن قيمة الدليل متروكة للقاضي بكامل سلطتة التقديرية دون تدخل من قبل المشرع.

وقد أخذت أكثر التشريعات بهذا النظام ، إذ أن القاضي يقدم الأدلة المقدمة إليه وفقاً لقناعاته

ويقوم بتقدير كل دليل على حده، والموازنة فيما بينهما، حتى يستخلص منها قرار البراءة أو الادانة[1].

وهنا يتقيد القاضي بالاصول التي تحددها النصوص التشريعية الى جانب تبني المنطق العلمي في البحث والتفتيش ، وعدم الإخلال بالإصول التي يفرضها القانون، ويخضع تقدير الأدلة لقاضي الموضوع دون رقابة من محكمة التمييز، ومع ذلك ، فإن هذه السلطة غير مطلقة ، فإذا خالف القاضي تقدير المنطق السليم، ولم يراعي الاستثناءات التي يفرضها المشرع ، عندئذ يجوز لها رد الذي اعتمده.

المطلب الثالث

العقوبات المقررة لجريمة التزوير الإلكتروني

إن بيان العقوبات المقررة في جريمة تزوير الإلكتروني يقتضي الرجوع إلى الصيغ التشريعية المجرمة لفعل التزوير ، سواء كان هذا الفعل مجرما بنصوص خاصة ، أو من خلال نصوص قانون العقوبات.

---

(1)بركات ، ميساء مصطفى ، جرائم التعدي على المعلوماتية الإتلاف و التزوير ، مرجع سابق ، ص108.

كما يقتضي الأمر أحيانا لتحديد العقوبة المناسبة، ربط النصوص الخاصة بنصوص قانون العقوبات في حال وجود عقوبات أشد منصوص عليها في هذا القانون.

وعليه سوف يتطرق الباحث عن العقوبات التي تصدر من التشريعات المقارنة لجريمة التزوير الإلكتروني وسيتناول الباحث في الفرع الأول عن العقوبات المقررة في التشريع المصري ، وكذلك في الفرع الثاني الذي خصصه الباحث عن العقوبات المقررة في التشريع الإماراتي ، وكذلك عن العقوبات المقررة في التشريع العراقي وهذا ما يبينه في الفرع الثالث ، أما الفرع الرابع يتناول العقوبات المقررة في التشريع الأردني.

الفرع الأول : العقوبات المقررة في قانون التوقيع الإلكتروني المصري :

عاقب المشرع المصري على فعل تزوير الإلكتروني بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه أو باحدى هاتين العقوبتين، وذلك في المادة 23 من قانون التوقيع الإلكتروني إلا أنه يجب مراعاة تطبيق العقوبة الأشد المنصوص عليها في قانون العقوبات أو أي قانون آخر[1].

ولذلك نصت هذه المادة على : " مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر، يعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه أو باحدى هاتين العقوبتين كل من : – أتلف أو عيب توقيعا أو وسيطا أو محررا الكترونيا أو زور شيئا من ذلك بطريق الإصطناع أو التعديل أو التحوير أو بأي طريق آخر".

---

(1)الرومي ، محمد أمين ، (2007) ، المستند الإلكتروني ، الطبعة الأولى ،دار الفكر الجامعي ، الإسكندرية ، ص85.

ولذلك يستنتج من هذا النص أن عقوبة تزوير المستند الإلكتروني في مصر تختلف بحسب نوع المستند الإلكتروني المزور[1].

فالتزوير في المحرر الإلكتروني الرسمي يعاقب عليه بعقوبة أشد ، و من ذلك التزوير الواقع في محرر من محررات الأحوال المدنية والتي لها طبيعة إلكترونية ، حيث اعتبرها المشرع المصري وثائق رسمية من خلال ما نص عليه في قانون الأحوال المدنية في المادة 72 منه، التي نصت على : " في تطبيق أحكام هذا القانون وقانون العقوبات تعتبر البيانات المسجلة بالحاسبات الآلية وملحقاتها بمراكز معلومات الأحوال المدنية ومحطات الإصدار الخاصة بها المستخدمة في إصدار الوثائق وبطاقات تحقيق الشخصية بيانات واردة في محررات رسمية".

فإذا وقع تزوير في المحررات السابقة أو غيرها من المحررات الرسمية تكون العقوبة الأشغال الشاقة المؤقتة أو السجن لمدة لا تقل عن خمس سنوات" .

ولذلك فإن عقوبة التزوير في المحرر الإلكتروني قد تكون هي العقوبة المنصوص عليها في المادة 23 من قانون التوقيع الإلكتروني، وقد تكون عقوبة أشد من الحبس والغرامة في حالات أخرى، وذلك إذا كان قانون العقوبات أو أي قانون آخر من قوانين الدولة يشدد العقوبة على تزوير مستند[2].

وهو مقتضى المادة (72) سابقة الذكر، حيث شددت العقوبة فيها إلى الأشغال الشاقة المؤقتة أو السجن لمدة لاتقل عن خمس سنوات، تبعا لطبيعة المحرر المزور.

---

(1)الرومي ، محمد أمين ، المستند الإلكتروني ، مرجع سابق ، ص87.

(2)الرومي ، محمد أمين ، المستند الإلكتروني ، مرجع سابق ، ص88.

غير أن الملاحظ أن المشرع الجنائي المصري لم يكن موفقا في تحديد العقوبة المناسبة لجريمة تزوير المحرر الإلكتروني باتخاذه منهجا معينا في العقاب، من خلال تلك النصوص المتفرقة بين قانون التوقيع الإلكتروني، وقانون العقوبات، وقوانين أخرى، مما جعل صيغة العقاب مجتزأة، فليس هناك نصاً جزائياً واحداً يبين تدرج العقوبة حسب طبيعة المحرر الإلكتروني المزور.

الفرع الثاني : العقوبات المقررة في قانون مكافحة الجرائم تقنية المعلومات الأماراتي:

نصت المادة (4) من قانون 2006/2 المتعلق بمكافحة جرائم تقنية المعلومات على:

يعاقب بالسجن المؤقت كل من زور مستندا من مستندات الحكومة الإتحادية أو المحلية أو الهيئات أو المؤسسات العامة الإتحادية والمحلية معترفا به قانونا في نظام معلومات وتكون العقوبة الحبس والغرامة أو إحدى هاتين العقوبتين إذا وقع التزوير فيما عدا ذلك من المستندات إذا كان من شأن ذلك إحداث ضرر".

لقد قرر المشرع الإماراتي لجريمة تزوير المحرر الرسمي الإلكتروني عقوبة السجن المؤقت كعقوبة أصلية ، سواء تعلق الأمر بالمحرر الصادر عن الحكومة الإتحادية أو المحلية باعتبارها تتمتع بقيمة قانونية ، وذلك عندما استخدم عبارة " معترفا به قانونا".

وفقاً للقاعدة العامة فإنه ينحسر مع هذه المادة إمكانية تطبيق المواد 217 و 217 مكرر، 222 من قانون العقوبات الإتحادي لوجود قانون خاص يعاقب على الفعل ذاته، إلا أن قانون مكافحة جرائم تقنية المعلومات قد نص في المادة 26 على: " لا يخل تطبيق العقوبات المنصوص عليها في هذا القانون بأية عقوبة أشد ينص عليها في قانون العقوبات أو أي قانون آخر "، وبذلك

يكون القانون رقم 02 لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات قد أحال إلى قانون العقوبات الإتحادي في تطبيق العقوبة متى كانت أشد من تلك الواردة فيه[1].

ليكون القاضي في جريمة التزوير الإلكتروني واستعماله ممسكا بالقانون رقم 2 لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات في يد وبقانون العقوبات الإتحادي في يد أخرى في معرض حكمه متحريا العقوبة الأشد الواردة في أي منهما ليقوم بتطبيقها على واقعة التزوير الإلكتروني[2].

وتعتبر عقوبة السجن المؤقت كعقوبة سالبة للحرية من العقوبات الملائمة بطبيعة وجسامة جريمة التزوير، باعتبار أن هذه العقوبات هي من العقوبات المقررة للجرائم المخلة بالثقة العامة.

أما بالنسبة للغرامة كعقوبة مالية فهي منصوص عليها في هذا القانون باعتبارها عقوبة اختيارية حيث يمكن الحكم بها مع عقوبة الحبس إذا تعلق الأمر بتزوير وثيقة معلوماتية غير رسمية ، وقد لايحكم بها[3].

كما نصت المادة 24 من نفس القانون على عقوبة المصادرة حيث نصت على : " مع عدم الإخلال بحقوق الغير حسن النية يحكم في جميع الأحوال بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا القانون أو الأموال

---

(1)أحمد عبد الواحد أحمد آل علي، (2011) ، جريمة التزوير في التوقيع الإلكتروني (دراسة مقارنة) ، رسالة لنيل درجة الماجستير في القانون الجنائي ، كلية القانون وعلوم الشرطة ، أكاديمية شرطة دبي ، ص142.

(2)أحمد عبد الواحد أحمد آل علي ، جريمة التزوير في التوقيع الإلكتروني (دراسة مقارنة) ، مرجع سابق ، ص142.

(3)حنان ، براهمي ،جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية ، مرجع سابق ، ص232.

المتحصلة منها ، كما يحكم بإغلاق المحل أو الموقع الذي يرتكب فيه أي من هذه الجرائم إذا كانت الجريمة قد ارتكبت بعلم مالكه ، وذلك إغلاقا كليا أو للمدة التي تقدرها المحكمة[1].

الفرع الثالث : العقوبات المقررة في مشروع قانون الجرائم المعلوماتية العراقي :

حيث نصت المادة (8) من مشروع قانون الجرائم المعلوماتية العراقي لسنة 2010 ، (يعاقب بالسحن المؤقت وبالغرامة لا تقل (10,000,000) عشرة ملايين دينار و لا تزيد على (15,000,000) خمسة عشر مليون دينار كل من ارتكب احد الأفعال:

أ- زور أو قلد أو اصطنع بنفسه أو بواسطة غيره توقيعاً أو سنداً أو كتابة إلكترونية أو شهادة تصديق أو ترخيص بمزاولة خدمات التوقيع الإلكتروني وما حكمها أو استعملها عمداً بشكل غير مشروع.

ب- زور أو قلد أو اصطنع بنفسه أو بواسطة غيره بأي شكل من الإشكال بطاقة الكترونية أو ذكية بأي وسيلة تستخدم في تحويل النقود المحلية والأجنبية المتداولة داخل العراق أو استخدامها أو روج لها أو تعامل بها وهو يعلم بعدم صحتها.

جـ - استعمل أو حاول استعمال البطاقة الإلكترونية المقلدة أو المزورة مع علمه بذلك ، أو قبل الدفع ببطاقة الوفاء المقلدة أو المزورة مع علمه بذلك.

---

(1)قانون مكافحة الجرائم تقنية المعلومات الأماراتي ، رقم 2 لسنة 2006 ، المادة (24).

د – إصطنع عمداً لنفسه أو لغيره أية بيانات أو وثائق أو سجلات أو قيود إلكترونية غير حقيقية أو أحدث أي تغيير أو تلاعب أو تحوير في أي سند إلكتروني أو استعمل أياً منها أمام أية جهة عامه أو خاصة[1].

هـ – صنع أو حاز بقصد البيع أو التوزيع أو العرض برامج أو اجهزة أو بيانات أو أية وسائل تقنية تستخدم في تزوير أو تقليد أو الاصطناع أو التحوير بقصد ارتكاب جناية أو جنحة.

نظم المشرع العراقي في هذه المادة المواضيع المتعلقة بالتزوير الإلكتروني حيث ذكر الصور المتعددة التي يقع عليها التزوير من ضمنها التوقيع والبطاقة الإلكترونية والمحرر وغيره، لكن إلى الأن لم يصدق عليه البرلمان العراقي وما زال هناك قصور تشريعي خصوصاً في هذا الموضوع.

الفرع الرابع: العقوبات المقررة في قانون الجرائم الإلكترونية الأردني :

أن قانون جرائم الإلكترونية الأردني رقم (27) لسنة 2015 أمكن تلمس معالجة جديدة لجريمة التزوير الإلكتروني في نصوص هذا القانون وتحديداً في المواد (3 ،4) التي ربطت المعنى بمصطلحات مثل " التعديل و التغيير " وهي كلمات تستوعب معنى التزوير اللفظي إلى حد بعيد حيث ترمي إلى تغيير حقيقة البيانات و المعلومات الإلكترونية دون أن تركز في قالبها[2].

(1)مشروع قانون الجرائم المعلوماتية العراقي لسنة 2010 ، المادة (8).

(2)المناعسة ، أسامة أحمد ، الزعبي ، جلال محمد ، جرائم تقنية نظم المعلومات الإلكترونية ، مرجع سابق ، ص169.

ولبيان صور الجريمة في هذا القانون نورد ما يلي :

1- الدخول المقصود إلى مو قع إلكتروني أو نظام معلومات بأي وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح إذا كان دخول بهدف تعديل أو تغيير بيانات أو ملعومات تقنية، حيث تورد الفقرة الثانية من المادة (3) من القانون على : **اذا كان الدخول المنصوص عليه في الفقرة (أ) من هذه المادة لالغاء او حذف او اضافة او تدمير او افشاء او اتلاف او حجب او تعديل او تغيير او نقل او نسخ بيانات او معلومات او توقيف او تعطيل عمل الشبكة المعلوماتية او نظام معلومات الشبكة المعلوماتية فيعاقب الفاعل بالحبس مدة لا تقل عن ثلاثة اشهر ولا تزيد على سنة وبغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) الف دينار أو بكلتا هاتين العقوبتين**[1].

2- أدخال أو نشر أو استخدام برامج تقنية قصداً في نظام تقنية معلومات أو شبكة اتصالات بهدف التعدي أو تغيير البيانات أو المعلومات التقنية ، وقد بينت المادة (4) من هذا القانون هذه المعاني فيما يلي : **يعاقب كل من ادخل او نشر او استخدم قصدا برنامجا عن طريق الشبكة المعلوماتية او باستخدام نظام معلومات بهدف الغاء او حذف او اضافة او تدمير او افشاء او اتلاف او حجب او تعديل او تغيير او نقل او نسخ او التقاط او تمكين الاخرين من الاطلاع على بيانات او معلومات او اعاقة او تشويش او ايقاف او تعطيل عمل نظام معلومات او الوصول اليه او تغيير موقع الكتروني او الغائه او اتلافه او تعديل محتوياته او اشغاله او انتحال صفته او انتحال شخصية مالكه دون تصريح او بما يجاوز او يخالف التصريح يعاقب بالحبس مدة لا تقل عن ثلاثة اشهر**

---
(1)قانون الجرائم الإلكترونية الأردني ، رقم 27 لسنة 2015 ، المادة(3).

ولا تزيد على سنة وبغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) الف دينار [1].

3- **اما في المادة الثامنة حيث نصت على : " تضاعف العقوبة على الجرائم المنصوص عليها في المواد من (3) الى (6) من هذا القانون بحق كل من قام بارتكاب أي منها بسبب تاديته وظيفته او عمله او باستغلال أي منهما**[2].

4- ويلاحظ في نصوص المادة (3 ، 4) أنها تميزت عن بعضها البعض في أسلوب الوصول إلى البيانات و المعلومات حيث نصت المادة الثالثة الدخول دون تصريح الى الشبكة المعلوماتية من أجل تغيير او تعديل البيانات ، أما المادة الرابعة نصت استخدام برامج تقنية واستخدامها من أجل التعدي أو التغيير أو التعديل في البيانات والمعلومات ونصت عقوبات لكل فعل صادر من الجاني من أجل ارتكاب الجريمة.

وبعد استعراض القوانين العربية التي التي عالجت الجرائم الإلكترونية والتزوير الإلكتروني بشكل خاص حيث تعتبر الإمارات هي من الدول السابقة في معالجة التزوير الإلكتروني ومن بعدها تأتي الدول العربية التي ذكرناها ، ومستمرة هذا الدول في المعالجة الجرائم الإلكترونية الى يومنا هذا ، وتطور هذه القوانين أدى إلى تطور التعامل بالمعاملات الإلكترونية ونتمنى أن يستمر هذا التطور.

---

(1)قانون الجرائم الإلكترونية الأردني ، رقم 27 لسنة 2015 ، المادة(4).

(2)قانون الجرائم الإلكترونية الأردني ، رقم 27 لسنة 2015 ، المادة (8)

الفصل الخامس

الخاتمة

في ختام هذه الدراسة نأمل ان نكون قد سلطنا الضوء على جريمة من اهم الجرائم الإلكترونية وهي جريمة التزوير الإلكتروني ، التي تدخل فيها الوسائل الالكترونية بشكل كبير ، وتتعاظم أهميتها كل يوم ، نظرا لانتشار استخدام المحررات الالكترونية على مستوى الأفراد والمؤسسات.

وتبين من خلال دراسة هذا الموضوع أن جرائم التزوير التي تقع على المحررات الالكترونية ، تهدد الثقة في التعامل بهذه المحررات وتمتد إلى تهديد الأشخاص ، من خلال شبكة الانترنت دون إمكانية تعرضهم للمساءلة القانونية كونهم في بلدان لا يعاقب فيها على مثل هذه الأفعال.

ومما تقدم نستنتج ان التزوير الذي يقع على المحررات الالكترونية ، لا يقل أهمية عن التزوير الذي يقع على المحررات الورقية لا سيما وان معظم القوانين العربية والأجنبية قد اعترفت بالحجية للمحرر الالكتروني بشكل مساوي للمحرر العادي.

ونأمل ان تكون دراستنا قد حققت الغرض المرجو منها ، باستعراض هذه الجريمة والمعالجات العملية التي أجراها التشريع الأردني و التشريعات المقارنة ، وكما هو معتاد فإن في ختام كل دراسة تظهر جملة من النتائج والتوصيات ومن اهمها ما يأتي:

اولاً : النتائج :

1- الجرائم الإلكترونية تمثل خطرا يوازي خطر الجريمة التقليدية ويفوقها في بعض الأحيان ، فقد تكون الأضرار التي تسببها الجريمة الإلكترونية اكبر بكثير من أضرار الجرائم التقليدية ، بالإضافة إلى صعوبة تقفي اثر المجرم الإلكتروني وبالتالي صعوبة القاء القبض عليه ، وفي كثير من الاحيان يكون المجرم الإلكتروني في مكان بعيد جدا عن موقع ارتكاب الجريمة فقد يكون في دولة أخرى أو حتى في قارة أخرى .

2- تتسم الجرائم الإلكترونية بخصائص فريدة تميزها عن الجرائم التقليدية سواء من جهة السلوك الاجرامي الذي هو سلوك تقني إلكتروني يرتكب في بيئة تقنية من حيث الطبيعة المعنوية للمحل الذي يقع عليه الاعتداء وكذلك النتيجة المترتبة عن هذا السلوك التي هي نتيجة معنوية تحدث في عالم افتراضي .

3- التزوير الذي يرد على المحررات الالكترونية بطرق إلكترونية يكون أكثر إتقان من التزوير بالطرق التقليدية ، ومن ثم فإن إمكانية اكتشافه تكون أكثر صعوبة .

4- اتبعت العديد من الدول نفس منهج قانون الأنسترال النموذجي للتجارة الإلكترونية لإزالة العقبات القانونية أمام التعامل بالمحرر الإلكتروني ، وهو ما سار عليه المشرع الأردني و الإماراتي ، والمصري ، والعراقي ، حيث تعتبر هذه التشريعات من النماذج العربية الأولى في تنظيم المعاملات الإلكترونية .

5- انتهج كل من المشرع الأردني و الإماراتي و المصري و العراقي منهجاً واحدا وهو تنظيم التعامل بالمحرر الإلكتروني في قانون مستقل ، وهو نفس نفس المنهج المتبع في تجريم تزوير الإلكتروني.

6- لم توفق هذه التشريعات في ضبط المصطلحات من الناحية القانونية والتقنية ، حيث تباينت المصطلحات المستخدمة في التعريف بالوثيقة المعلوماتية بين مصطلح السجل الإلكتروني ، المستند الإلكتروني، رسالة المعلومات ، على خلاف قانون الأونسترال النموذجي الذي استخدم مصطلح رسالة البيانات.

7- فتحت هذه التشريعات المجال أمام استخدام المحرر الإلكتروني في المعاملات الرسمية و الغير الرسمية ، ولدى المؤسسات والدوائر الحكومية أو بين الأفراد ، مما استوجب حماية المحرر سواء كانت رسمية أو خاصة بين الأفراد ضد أشكال الإعتداءات والجرائم الماسة بها ، ومن بينها التزوير.

8- انتهج المشرع الفرنسي منهجاً مغايرا للنماذج التشريعية السابقة ، حيث جسد مبدأ النظير الوظيفي في التعامل بالمحرر الإلكتروني -- وهو مبدأ الذي قرره قانون الأنسترال – من خلال تحقيق الإنسجام بين النصوص القانونية القائمة و المتطلبات التكنولوجية، لتحقيق المقصد من تجريم التزوير الإلكتروني.

9- تقوم جريمة تزوير التوقيع الإلكتروني بأفعال مختلفة عن تزوير التقليدي من خلال الحصول على منظومة التوقيع بطريقة غير شرعية بنية استخدامها في توقيع المحرر ، أو من خلال كسر الشفرة ، أما تزوير البطاقة الائتمانية بتلاعب في كيانها الإلكتروني ، كما

هو الحال بالنسبة لكيانها المادي ، بل إن تزويرها لن يتم بشكل مستقل عن التلاعب في تلك المعلومات المشفرة الموجودة عليها.

10- ضعف في الخبرة التقنية التي يمتلكها الضابط العدلية في تقصي الجريمة والكشف عن الجاني ، وكذلك قلة الأجهزة التي تساعده في تتبع الجاني الإلكتروني .

11- يتذيل العراق الدول التي عالجت الجرائم الإلكترونية إذ إنه ولهذه اللحظة قام بأصدار مشروع قانون الجرائم المعلوماتية لسنة 2010، ولم يصادق إلى الأن البرلمان العراقي على هذا المشروع من أجل مواكبة الدول وأيصاً من أجل محاربة مثل تلك الجرائم ، بإستثناء قانون التوقيع الالكتروني رقم 87 لسنة 2012 رغم ما يحويه قصور تشريعي .

ثانيا : التوصيات :

1- إعتماد مبدأ النظير الوظيفي في الصيغ التشريعية لإمكانية التعامل بالمحرر الإلكتروني مقارنة بالمحرر الورقي ، ومساواتها بها من حيث القيمة القانونية في الإثبات ، من خلال الإسترشاد بما نص عليه قانون الأونسترال في هذا المجال خاصة ما يتعلق بتحقيق هذا المبدأ من الناحية التقنية.

2- العمل على الاقتداء بالدول المتقدمة والتعاون معها في مجال التكنولوجيا والاستفادة من خبراتها في تشريع القوانين التي تعالج جرائم الإلكترونية ، كونها صاحبة باع طويل في مكافحة مثل هذه الجرائم ، ولاننا نعلم انه ما من دولة يمكنها النجاح في مواجهة هذه الانماط المستحدثة بمفردها دون تعاون وتنسيق مع غيرها من الدول في مجال المساعدات

القضائية ، وتسليم المجرمين ، وتدريب الكوادر البشرية ، وهذا ما نصت عليه العديد من الاتفاقيات الدولية.

3- تجنب الصيغة التشريعية التي تصنف جريمة تزوير الإلكتروني ضمن جرائم المساس بالأنظمة الإلكترونية ، وذلك لإختلاف المصلحة المحمية جزائياً ، حيث المصلحة المعتبرة في جريمة التزوير هي حماية الثقة العامة في المحرر لاسيما المحرر الرسمي الصادرة عن الجهات الإدارية ، بينما المصلحة المعتبرة في جرائم المساس بالأنظمة الإلكترونية هي حماية النظام.

4- ضبط صيغة التجريم من حيث بيان النية الإجرامية المطلوبة ، وهي نية الغش في تغيير الحقيقة اضراراً بالغير ، كما أشارت إلى اتفاقية بودابست حول الإجرام الإلكتروني.

5- العمل على انشاء جهاز امني مختص في مكافحة جرائم المعلوماتية يختص بالبحث والتقصي عن مجرمي المعلوماتية ، والعمل على توفير المساعدات التقنية والتدريب لهذا الجهاز لدعم رجال الشرطة والمحققين والقضاة ، فيصبح الجهاز التحقيقي بذلك اكثر فعالية في مكافحة مثل هذه الجرائم ، ومتابعة المجرمين عبر شبكات الانترنت وتقفي اثارهم والقاء القبض عليهم .

6- تحديد الشروط التقنية اللازمة في التوقيع الإلكتروني المقترن بالمحرر الإلكتروني ، كي تتمتع هذه الأخيرة بالحماية القانونية اللازمة ضد التزوير ، ولضمان المحرر عند التعامل به ، لاسيما إذا كان هذا المحرر صادرة عن جهات إدارية عامة، ويعتبر التوجيه الأوربي

للتوقيع الإلكتروني نموذجا في هذا المجال، حيث ميز بين التوقيع الإلكتروني البسيط ، والتوقيع الإلكتروني المتقدم الذي يمنح قيمة قانونية أقوى للمحرر الإلكتروني.

7- يحتاج القاضي الجزائي للحكم بوجود تزوير في المحرر الإلكتروني إلى خبراء متخصصين في كشف أساليب التزوير الإلكتروني ، وتتبع أثر التزوير في هذا المحرر ، أضافة إلى تدريب القاضي على مثل تلك الأمور.

8- أدعو المشرع الأردني و العراقي وكافة التشريعات المقارنة مراعاة الأساليب المستخدمة في التزوير الإلكتروني باعتبارها لا تترك أثرا ظاهرا ، حيث تتم بأساليب تقنية فنية، وبالتالي يحتاج الأمر لجهاز تقني متخصص في تتبع الدليل لكشف التزوير الإلكتروني.

قائمة المراجع

أولاً : الكتب و المؤلفات :

- إبراهيم ، خالد ممدوح ، (2009) ، **التحكيم الإلكتروني في عقود التجارة الدولية** ، طبعة الأولى ، دار الفكر الجامعي ، الإسكندرية.
- أحمد ، هلالي عبد الإله ، (2003) ، **الجوانب الموضوعية والإجرائية لجرائم المعلوماتية** ، الطبعة الأولى ، دار النهضة العربية ، القاهرة.
- أسامة سمير حسين ،(2011)،**الإحتيال الإلكتروني الوجه القبيح للتكنولوجيا** ،الطبعة الأولى ، الجنادرية للتوزيع ،الأردن ، عمان.
- البرادعي ، أحمد بن عبد الله ، (1995) ، **معاينة الجريمة بين النظرية و التطبيق** ، **مطابع ينبع الحديثة** ، المملكة العربية السعودية.
- بصلة ، رياض فتح الله ، (1995) ، **جرائم بطاقات الإئتمان** ، الطبعة الأولى ، دار الشروق ، القاهرة.
- جميعي ، حسن عبد الباسط ،(2000)،**إثبات التصرفات القانونية التي يتم إبرامها عن طريق الإنترنيت** ، دار النهضة العربية ، القاهرة.
- الجنبيهي ، منير محمد ، والجنبيهي ، ممدوح محمد ،(2004) ، **التوقيع الإلكتروني وحجيته في الإثبات** ، دار الفكر الجامعي، القاهرة.

- حجازي ، عبد الفتاح بيومي ، (2002) **الدليل الجنائي والتزوير في جرائم الكومبيوتر والانترنت** ، دار الكتب القانونية، القاهرة.
- حجازي ، عبد الفتاح بيومي ، (2005)، **جريمة غسل الأموال بين الوسائط الإلكترونية ونصوص التشريع**،الطبعة الاولى،دار الفكر الجامعي،الإسكندرية.
- حجازي ، عبد الفتاح بيومي ، (2007)، **الجريمة في عصر العولمة** ، الطبعة الأولى، دار الفكر الجامعي ، الإسكندرية.
- حجازي ، عبد الفتاح بيومي ،(2004)،**التجارة الإلكترونية وحمايتها القانونية**،الطبعة الاولى،دار الفكر الجامعي،القاهرة.
- حجازي ، عبد الفتاح بيومي ، (2004) ، التوقيع الإلكتروني في النظم القانونية المقارنة،الطبعة الأولى ، دار الفكر الجامعي ، الإسكندرية.
- حجازي ، عبد الفتاح بيومي ،(2007)،**النظام القانوني للتوقيع الإلكتروني**،الطبعة الأولى،دار الكتب القانونية،مصر ،المحلى الكبرى.
- حجازي ، عبد الفتاح بيومي ،(2007)،**مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنيت** ، دار الكتب القانونية ، المحلة الكبرى ، مصر.
- حجازي ، عبد الفتاح بيومي ،(2008)،**تزوير في جرائم الكمبيوتر والإنترنيت**،دار الكتب القانونية،المحلة الكبرى السبع بنات ، مصر.

- حسبو ، أحمد عمرو ،(2000)،**حماية الحريات في مواجهة نظم المعلومات** ، الطبعة الأولى ، دار النهضة العربية ، القاهرة.
- حسن ،إيهاب فوزي ، (2006) ،**الحماية الجنائية والأمنية لبطاقات الائتمان** ، أطروحة دكتوراه مقدمة إلى أكاديمية الشرطة في مصر.
- حسني، محمود نجيب ،(1988)، **شرح قانون العقوبات ، القسم الخاص**، دار النهضة، القاهرة .
- د . فوزية ، عبد الستار ،(1988)،**شرح قانون العقوبات ، القسم الخاص**، دار النهضة العربية ،القاهرة.
- د. السعيد ، مصطفى السعيد ، (2000) ، **قانون عقوبات القسم العام** ، دار النهضة العربية ، القاهرة.
- د. رستم، هشام محمد فريد،(1995)،**قانون العقوبات ومخاطر تقنية المعلومات**،الطبعة الأولى،مكتبة الآلات الكاتبة،أسيوط.
- د. عوض محمد،(1984)، **جرائم الأشخاص والأموال**، دار المطبوعات الجامعية، الإسكندرية.
- د.فخري،محمد صالح عثمان ، (1995) ، **جرائم بطاقة الائتمان**،الطبعة الأولى، دار الشروق ،القاهرة.

- رمضان، عمر السعيد ،(1965)،**شرح قانون العقوبات** ، القسم الخاص،الطبعة الأولى، القاهرة ،دار النهضة العربية.

- الرومي ، محمد أمين، (2008)، **النظام القانوني للتوقيع الإلكتروني**،دار الكتب القانونية ، مصر.

- زين الدين، بلال امين، (2008)،**جرائم نظم المعالجة الالية للبيانات**،الطبعة الاولى،دار الفكر الجامعى،الاسكندرية.

- سرور ، أحمد فتحي ، (1995) ، **الشرعية الدستورية وحقوق الإنسان في الاجراءات الجنائية** ، الطبعة الأولى ، دار النهضة العربية ، القاهرة.

- سعد،عبد العزيز،(2005)،**جرائم التزوير وخيانة الأمانة واستعمال المزور**،الطبعة الاولى،دار هومة،الجزائر.

- سليم ، أيمن سعيد ، (2004)،**التوقيع الإلكتروني**،الطبعة الأولى،دار النهضة العربية ، القاهرة.

- الشاوي ، توفيق ، (1954) ، **فقه الاجراءات الجنائية** ، دار الكتاب العربي ، القاهرة.

- شمس الدين ، أشرف توفيق ،(2006)،**الحماية الجنائية للمستند الإلكتروني** ، الطبعة الأولى ، دار النهضة العربية ، القاهرة.

- الصغير ، جميل عبد الباقي ، (2001) ، **الجوانب الإجرائية للجرائم المتعلقة بالإنترنت**، دار النهضة العربية ، القاهرة.

- الصغير ، جميل عبد الباقي ،(1999)، **الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة** ،الطبعة الأولى ، دار النهضة العربية ، القاهرة.
- صوالحة، معادي اسعد ، (2011) ، **بطاقات الائتمان النظام القانوني واليات الحماية الجنائية و الأمنية** – دراسة مقارنة ، المؤسسة الحديثة ، لبنان.
- الصيفي ، عبد الفتاح ، دون سنة طباعة ، **أصول المحاكمات الجزائية** ، دار النهضة العربية ، مصر.
- عالية ، سمير ، (1996) ، **أصول قانون العقوبات** ، القسم العام ، الطبعة الأولى ، المؤسسة الجامعية للدراسات والنشر و التوزيع ، بيروت.
- العبادي ، محمد حميد الرصفان ، (2015) ، **الجرائم المستحدثة في ظل العولمة** ، الطبعة الاولى ، دار جليس الزمان ، عمان.
- عباس ، حسن عبد الله ، التوقيع الإلكتروني ، (2003) ، **التوقيع الإلكتروني**، المجلد التاسع عشر ، مجلة العلوم الإقتصادية و الإدارية ، الكويت.
- عبد الباقي ، جميل ،(2001) ، **الانترنت والقانون الجنائي** ،الطبعة الأولى ، دار الفكر العربي ، القاهرة.
- عبد الحكيم ، سامح محمد ، (2003) ، **الحماية الجنائية لبطاقات الائتمان** ، دار النهضة العربية ، القاهرة.

- عبد الحميد، ثروت ،(2002)،**التوقيع الإلكتروني** ،الطبعة الثانية ، مكتبة الجلاء الجديدة بالمنصورة ، مصر.

- عبد الستار ، فوزية ، (1986) ، **شرح قانون الاجراءات الجنائية** ، دار النهضة العربية، القاهرة.

- عبد العال ، محمد حسين ، (1999)،**ضوابط الإحتجاج بالمستندات العقدية في القضاء الفرنسي** ،الطبعة الأولى ، دار النهضة العربية ، القاهرة.

- عبيد ، دكتور رؤوف ، (2016) ، **جرائم التزييف والتزوير** ، الطبعة الاولى ، مكتبة الوفاء القانونية ، الاسكندرية.

- عبيدات ، لورنس محمد ، (2005) ، **اثبات المحرر الالكتروني** ، الطبعة الأولى ، ، دار الثقافة للنشر والتوزيع ، عمان.

- العزام، سهيل محمد ،(2009)، **التوقيع الإلكتروني**،الطبعة الأولى ، المكتبة الوطنية ، عمان.

- عفيفي،كامل عفيفي،(2007)،**جرائم الكمبيوتر وحقوق الؤلف والمصنفات الفنية ودور الشرطة والقانون**،الطبعة الثانية،منشورات الحلبي الحقوقية،بيروت.

- عيسى ، طوني ميشال ، (2001) ، **التنظيم القانوني لشبكة الإنترنت** ، الطبعة الأولى، منشورات صادر الحقوقية ، بيروت.

- الغريب ، محمد عيد ، (1997) ، **حرية القاضي الجنائي في الإقتناع اليقيني و أثره في تسبيب الأحكام الجنائية** ، الطبعة الأولى ، النسر الذهبي للطباعة والنشر ، القاهرة.
- فهمي ، خالد مصطفى ، (2007)،**النظام القانوني للتوقيع الإلكتروني في ضوء الإتفاقيات الدولية والتشريعات العربية** ، الطبعة الأولى ، دار الجامعة الجديدة ، الإسكندرية.
- القهوجي, علي عبد القادر, (2002), **جرائم الاعتداء على المصلحة العامة وعلى الانسان والمال** – القسم الخاص – منشورات الحلبي الحقوقية، بيروت.
- قورة ، نائلة عادل محمد فريد ،(2005)،**جرائم الحاسب الآلي الإقتصادي** ، الطبعة الأولى ، منشورات حلبي الحقوقية ، بيروت.
- ماهر عبد شويش الدرة ،(2002)، **شرح قانون العقوبات – القسم الخاص –** ، دار الفكر الجامعي ، القاهرة.
- مرهج ، محمد حماد ، (2009) ، **الحماية الجنائية لبطاقات الائتمان الممغنطة** ، دار الكتب القانونية ،مصر.
- المشهداني ، محمد أحمد ،(2001)،**شرح قانون العقوبات، القسم الخاص**،الطبعة الأولى،عمان.
- مصطفى ، أحمد محمود ،(2010)، **جرائم الحاسبات الإلية في التشريع المصري**، الطبعة الأولى ، دار النهضة العربية ، القاهرة.

- المناعسة ، أسامة أحمد ، والزعبي جلال محمد ، (2014) ، **جرائم تقنية نظم المعلومات الإلكترونية (دراسة مقارنة)** – دار الثقافة ، عمان.
- المهيري ، خالد محمد كدفور، **جرائم الكمبيوتر والإنترنيت والتجارة الإلكترونية** ، الطبعة الثانية ، معهد القانون الدولي ، دبي .
- النقيب ، عاطف ، (1986) ، **أصول المحاكمات الجزائية** ، دراسة مقارنة ، منشورات عويدات ، بيروت.
- يونس عرب , (2002) ، **دليل أمن المعلومات والخصوصية – جرائم الكمبيوتر والانترنيت،** الطبعة الاولى، اتحاد المصارف العربية ، الجزء الاول، عمان.

ثانياً : الرسائل العلمية :

- أحمد عبد الواحد أحمد آل علي، (2011) ، **جريمة التزوير في التوقيع الإلكتروني (دراسة مقارنة)** ، رسالة لنيل درجة الماجستير في القانون الجنائي ، كلية القانون وعلوم الشرطة ، أكاديمية شرطة دبي.
- براهمي ، حنان ، (2014) ، **جريمة التزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية** ، أطروحة لنيل شهادة الدكتوراه ، جامعة محمد خضير بسكرة ، كلية الحقوق والعلوم السياسية ، جزائر.

- بركات ، ميساء مصطفى ، (2006) ، **جرائم التعدي على المعلوماتية الإتلاف و التزوير** ، رسالة لنيل شهادة الماجستير ، جامعة بيروت العربية ، كلية الحقوق ، بيروت.
- حسن ،إيهاب فوزي ، (2006) ،**الحماية الجنائية والأمنية لبطاقات الائتمان** ، أطروحة دكتوراه مقدمة إلى أكاديمية الشرطة في مصر.
- الحكيمي ، عبد الباسط محمد سيف ، (2000) ، **النظرية العامة للجرائم ذات الخط العام** ، أطروحة لنيل شهادة الدكتوراه ، بغداد.
- السراني ، عبد الله بن مسعود محمد ، (2011) ، **فعالية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني** ، رسالة لنيل شهادة الماجستير، جامعة نايف العربية للعلوم الأمنية ، الرياض.
- الكعبي ، محمد عبيد ، (2009) ، **الحماية الجنائية للتجارة الالكترونية** ، أطروحة لنيل شهادة الدكتوراه ، كلية الحقوق ، جامعة القاهرة.
- السوداني ، مثنى سعد جبار ، (2013) ، **التزوير المعلوماتي في الحاسب الآلي** ، رسالة لنيل شهادة الماجستير ، الجامعة المستنصرية ، بغداد.
- طنطاوي ، ابراهيم حامد مرسي ، (1997) ، **سلطات مأمور الضبط القضائي** – دراسة مقارنة -- ، أطروحة لنيل شهادة الدكتوراه ، المكتبة القانونية ، القاهرة.
- عباس ، حفصي ، (2014) ، **جرائم التزوير الإلكتروني** ، أطروحة لنيل شهادة الدكتوراه ، جامعة وهران ، كلية العلوم الأنسانية و العلوم الأسلامية ، الجزائر.

- فهد ، بن سعد بن عبدالله ، (1996) ، **الأحكام الشرعية و النظامية لجرائم تزوير المحررات الرسمية** ، رسالة لنيل شهادة الماجستير ، المعهد العالي للعلوم الأمنية ، الرياض.

- قفطان ، محمد عايد ، (2014) ، **القصد الجرمي في تزوير التوقيع الإلكتروني** ، رسالة لنيل شهادة الماجستير ، جامعة جدارا ، الأردن.

- محمود ، لمى عامر ، (2008) ، **الحماية الجنائية لرسائل الاتصال** -- دراسة مقارنة – أطروحة لنيل شهادة الدكتوراه ، كلية القانون ، جامعة بابل ، العراق .

ثالثاً : البحوث في المجلات و الدوريات و المحاضرات و المؤتمرات :

- د. زين محمد الزماني، (1421 هـ) ، **التزوير والتزييف عن طريق بطاقات الائتمان،** مجلة المحامي، ع3، الرياض ، ص52.

- رستم ، هشام محمد فريد ، (1999) ، **الجرائم المعلوماتية** ، أصول التحقيق الجنائي و الفني و آلية التدريب الشخصي للمحققين ، مجلة الأمن والقانون ، السنة السابعة ، العدد الثاني.

- شكري ، عادل يوسف ، (2008) ، **الجريمة المعلوماتية و أزمة الشرعية الجزائية** ، مجلة الجريمة المعلوماتية ، العدد السابع .

- العقايلة ، زيد محمود ، **حجية الرسائل المرسلة عن طريق الهاتف المحمول في أثبات التعاقد** ، بحث مقدم في مؤتمر المعاملات الإلكترونية في الإمارات ، دبي.

- علي محمود علي حموده،(2003) ،**الادلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي** ، بحث منشور ضمن أعمال مؤتمر الجوانب القانونية و الأمنية للعمليات الإلكترونية ، أكادمية شرطة دبي , المجلد الأول.
- القهوجي ، علي عبد القادر ، (1992) ، **الحماية الجنائية لبرنامج الحاسوب** ، بحث منشور لمجلة الحقوق للبحوث القانونية والأقتصادية ، كلية الحقوق ، جامعة الإسكندرية.
- القهوجي ، علي عبد القادر ، (2000) ، **الحماية الجنائية للبيانات المعالجة إلكترونياً** ، بحث مقدم إلى مؤتمر القانون و الكمبيوتر و الإنترنت ، كلية الشريعة والقانون ، جامعة الإمارات العربية المتحدة.
- مجلة المحقق الحلي للعلوم القانونية والسياسية ، **تزوير المعلوماتي لبطاقة الائتمان** ، العدد الثاني ، السنة السابعة.
- مؤتمر عن الحكومة الالكترونية ، المركز التجاري بدبي للفترة من 21 – 22 / 1 / 2000م وتطرق المؤتمر الى **التحقيق الجنائي الالكتروني ومشكلاته العملية** .
- اليوسف ، عبد العزيز ، (1992) ، **تقنية في الجرائم المستحدثة** ، بحث ضمن منشورات أكادمية نايف العربية للعلوم الأمنية ، الإمارات.
- يونس عرب ، (2002) ، **جرائم الكمبيوتر و الإنترنت** ، ورقة عمل مقدمة إلى مؤتمر الأمن العربي ، تنظيم المركز العربي للدراسات و البحوث الجنائية ، أبو ظبي.

رابعاً : القوانين :

1 –القوانين الأردنية :

- قانون العقوبات الأردني رقم 16 لسنة 1960.
- قانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015.
- قانون المعاملات الإلكترونية الأردني رقم 15 لسنة 2015.

2–القوانين العراقية :

- قانون التوقيع الإلكتروني و المعاملات الإلكترونية العراقي ، رقم78 ، لسنة 2012.
- قانون العقوبات العراقي رقم 111 لسنة 1969.
- مشروع قانون الجرائم المعلوماتية العراقي لسنة 2010.

3–القوانين العربية :

- قانون الأحوال المدنية المصري رقم 143 لسنة 1994.
- قانون التوقيع الإلكتروني المصري رقم 15 لسنة 2004.
- قانون مكافحة جرائم التقنية المعلومات الإماراتي رقم 2006/2 لسنة 2006.
- مشروع قانون التجارة الإلكترونية المصري لسنة 2010.

4–القوانين الأجنبية :

- قانون العقوبات الفرنسي لسنة 1992.

خامساً : القررات ومجموعة الاحكام والمعاهدات والمقالات الإلكترونية :

- قانون الأونسترال النوذجي للتحكيم التجاري الدولي ، لسنة 1985.
- الجهني ، أمجد حمدان ، جرائم بطاقة الدفع الإلكتروني عبر شبكة الانترنيت ، (http://www.cojss.com /replay.php?a=219)).
- كردي ، أحمد السيد، توقيع الإلكتروني مفهومه التكنولوجي وحمايته ، 30 سبتمبر 2011، (http://kenanaonline.com/users/ahmedkordy/posts/323677)
- مجموعة احكام النقض المصرية .
- مجموعة القواعد القانونية المصرية.
- الكردي ، علي عواد ، الحماية الجزائية في جريمة انتهاك مراسلات البريد الإلكتروني (https://www.dorar-aliraq.net/threads/597027).